Security made simple.

Sophos UTM

管理ガイド

製品バージョン: 9.300

文書作成日：2015年2月11日

http://www.sophos.com

限定保証

当文書に記載されている情報の正確性は保証されません。コメントや修正については、nsg-docu@sophos.comまでご連絡ください。

目次

1 インストール

このセクションは、ネットワークへのSophos UTMのインストールとセットアップについての情報を提供します。Sophos UTMのインストールは、2つのステップで行います。まずソフトウェアをインストールし、次に基本システム設定を行います。ソフトウェアのインストールに必要な初期セットアップは、コンソールベースのインストールメニューで行います。内部設定は、管理ワークステーションで、Sophos UTMのWebベースの管理用インタフェースであるWebAdminを使用して実行できます。インストールを開始する前に、ハードウェアがシステムの最低要件を満たしていることを確認してください。

注 – ハードウェアアプライアンスを使用する場合、次のセクションをスキップして、Sophos UTM*基本設定*のセクションに直接進むことができます。この理由は、すべてのハードウェアアプライアンスはSophos UTMソフトウェアがプレインストールされた状態で出荷されるためです。UTM

この章には次のトピックが含まれます。

- 参考資料
- システム要件
- インストール手
- 基本設定
- バックアップリストア

1.1 参考資料

インストールを始める前に、Sophos UTM製品の設定の一助となる以下のマニュアルを読むことをお勧めします。いずれのマニュアルも、Sophos UTMハードウェアアプライアンス装置に同梱されています。また、Sophos UTMリソースセンターでもご利用いただけます。

- クイックスタートガイドハードウェア
- 取扱説明書

1.2 システム要件

UTMのインストールおよび使用のための最低限のハードウェア要件は以下のとおりです。

- プロセッサ：Intel Atom Dual Core（1.46GHz）（あるいは互換のもの）
- メモリ：2 GB RAM
- **HDD**：40 GB SATAハードディスクドライブまたはSSD
- **CD-ROM** ドライブ：ブート可能なIDEまたはSCSI CD-ROMドライブ
- **NIC**：2枚以上のPCI 2.0イーサネットネットワークインタフェースカード
- **NIC**（オプション）：1枚のハートビート対応PCIイーサネットネットワークインタフェースカード。冗長化システムでは、プライマリシステムとセカンダリシステムが、いわゆるハートビート要求を介して互いに通信します。冗長化システムをセットアップする場合は、両方のユニットにハートビート対応のネットワークインタフェースカードを装備する必要があります。
- **USB**（オプション）：UPSデバイスとの通信用のUSBポート1つ、およびSophos UTMSmart Installer（SUSI）接続用のUSBポート1つ
- スイッチ(オプション) ：ネットワークセグメントの接続（およびその間の選択）を行うネットワークデバイス。このスイッチはジャンボフレームをサポートすることが必要です。

Sophosでは、UTMソフトウェアと互換性を持つハードウェアデバイスのリストを用意しています。*ハードウェア互換性リスト*(HCL)はSophos Knowledgebaseからご利用いただけます。UTMソフトウェアのインストールと使用でエラーの発生を防止するために、HCLにリストされたハードウェアのみを使用してください。WebAdminへのアクセスに使用されるクライアントPCに必要なハードウェアおよびソフトウェアの条件を以下に示します。

- プロセッサ：クロック周波数：2GHz以上
- ブラウザ：最新バージョンのFirefox（推奨）、最新バージョンのChrome、最新バージョンのSafari、またはMicrosoft Internet Explorer 8以降。JavaScriptを有効にする必要があります。さらに、UTMの内部ネットワークカードのIPアドレス（eth0）にプロキシを使用しないようにブラウザを設定する必要があります。

1.2.1 UPSデバイスのサポート

無停電電源装置（UPS）デバイスは、公共の電力が利用できない場合に、別個の電源から接続した機器に電力を供給して給電を維持します。Sophos UTM は、MGE UPS SystemsおよびAPCのUPSデバイスをサポートしています。UPS デバイスとSophos UTMの通信はUSBインタフェースを介して行われます。

UPS デバイスがバッテリオペレーションを始動すると、管理者に通知が送信されます。停電が長期間続いて UPS デバイスの電圧が限界値に近づいた場合は、管理者に別のメッセージが送信されます。そして、Sophos UTMは自動的にシャットダウンします。

注 – Sophos UTMにUPSデバイスを接続するときは、UPSデバイスの使用説明書をお読みください。UTMのUSB インタフェースを介してブート(起動)すると、UTM は UPS デバイスを認識します。USB インタフェースを相互に接続してからSophos UTMをブートしてください。

1.2.2 RAIDサポート

RAID(Redundant Array of Independent Disks)とは、複数のハードドライブを使用してドライブ間でデータを共有あるいは複製するデータストレージ技術です。RAID システムが検出されてダッシュボードに正しく表示されるようにするには、Sophos UTMでサポートされる RAID コントローラを使用することが必要です。サポートされている RAID コントローラを確認するには、HCL をチェックしてください。HCL はSophos Knowledgebaseで提供されています。「HCL」を検索用語として使用して、該当するページを探してください。

1.3 インストール手順

次に、Sophos UTMソフトウェアのインストールプロセスを順を追って説明します。

インストールを始める前に、次のアイテムがお手元にあることを確認してください。

- Sophos UTMCD-ROM
- 用のライセンスキーSophos UTM

セットアッププログラムがシステムのハードウェアをチェックしてから、PCにソフトウェアをインストールします。

1.3.1 インストール中の主な機能

メニューのナビゲーションには、次のキーを使用します(画面の下部にも追加のキー機能がリストされています)。

- F1:コンテキストに応じたヘルプ画面が表示されます。
- カーソルキー:これらのキーを使用して、テキストボックス間をナビゲーションします(たとえば、ライセンス条件や、キーボードレイアウトの選択時)。
- Tabキー:テキストボックス、リスト、ボタンを前後に移動します。
- Enterキー:入力した情報が確定され、インストールが次のステップに進みます。
- Spaceキー:アスタリスク(*)の付いたオプションを選択または選択解除します。

- Alt-F2:インストールコンソールに切り替えます。
- Alt-F4:ログに切り替えます。
- Alt-F1:インタラクティブバッシュシェルに切り替えます。
- Alt-F1:メインのインストール画面に戻ります。

1.3.2 インストール中の特別なオプション

一部の画面には追加のオプションがあります。

ログの閲覧:インストールログを開きます。

サポート:サポートダイアログ画面を開きます。

USBスティックへ:インストールログをzipファイルとしてUSBスティックへ書き込みます。このオプションを確定する前に、必ずUSBスティックを差し込んでください。このzipファイルは、インストールでの問題をSophos UTMサポートチームなどが解決する際に使用されます。

戻る:前の画面に戻ります。

キャンセル:インストールの中止を確認するダイアログウィンドウが開きます。

ヘルプ:コンテキストに応じたヘルプ画面が開きます。

1.3.3 Sophos UTMのインストール

1. **CD-ROMドライブからPCを起動します。または、ダウンロードしたISOを仮想ドライブに搭載します。**
   インストール開始画面が表示されます。

   > 注 – いつでもF1を押してヘルプメニューを利用することができます。開始画面でF3を押すと、トラブルシューティングの画面が開きます。

2. **Enterを押します。**
   *開始*画面が表示されます。
3. ***インストール開始*を選択します。**
   *ハードウェア検出*画面が表示されます。

   ソフトウェアが次のハードウェアコンポーネントをチェックします。

- CPU
- ハードディスクドライブのサイズと型
- CD-ROMドライブ
- ネットワークインタフェースカード
- IDEまたはSCSIコントローラ

システムが最低要件を満たしていない場合、エラーが報告され、インストールは中止されます。

ハードウェア検出が完了すると、*検出されたハードウェア*画面が参考として表示されます。

4. **Enterを押します。**
   *キーボード選択*画面が表示されます。
5. **キーボードのレイアウトを選択します。**
   カーソルキーを使用してキーボードレイアウト(例:*English (UK)*)を選択し、Enterを押して続行します。

   *タイムゾーン選択*画面が表示されます。
6. **エリアを選択します。**
   カーソルキーを使用してエリア(例:*Europe*)を選択し、Enterを押して続行します。
7. **タイムゾーンを選択します。**
   カーソルキーを使用してタイムゾーン(例:*London*)を選択し、Enterを押して続行します。

   *日付と時刻*画面が表示されます。
8. **日付と時刻を設定します。**
   日付と時刻が正しくない場合、ここで変更できます。Tabキーとカーソルキーを使用して、テキストボックス間を切り替えます。*ホストクロックはUTC*オプションの選択を解除するには、Spaceキーを押します。無効なエントリは却下されます。設定をEnterキーで確認します。

   *管理インタフェース選択*画面が表示されます。
9. **内部ネットワークカードを選択します。**
   WebAdminツールを使用してSophos UTMの残りの設定を行う場合、内部ネットワークカード(eth0)とするネットワークインタフェースカードを選択します。リストから使用可能なネットワークカードを1つ選択し、Enterキーで選択を確認します。

   > 注 – アクティブな接続があるインタフェースは、*[link]*と表示されます。

*ネットワーク設定*画面が表示されます。

10. **管理ネットワークインタフェースを設定します。**
管理ネットワークインタフェースとする内部インタフェースのIPアドレス、ネットワークマスク、ゲートウェイを定義します。デフォルト値は以下のとおりです。

アドレス: `192.168.2.100`

ネットマスク: `255.255.255.0`

ゲートウェイ: なし

ネットマスクで定義されたサブネット外にあるワークステーションからWebAdminインタフェースを使用したい場合のみ、ゲートウェイ値を変更する必要があります。ゲートウェイ自体がサブネット内にある必要があります。[1]

設定をEnterキーで確認します。

CPUが64ビットをサポートしている場合、*64ビットカーネルのサポート*画面が表示されます。サポートしていない場合、続いて*Enterprise Toolkit*画面が表示されます。

11. **64ビットカーネルをインストールします。**
*はい*を選択すると64ビットカーネルが、*いいえ*をインストールすると32ビットカーネルがインストールされます。

*Enterprise Toolkit*画面が表示されます。

12. **Enterprise Toolkitのインストールに同意します。**
Enterprise ToolkitはSophos UTMソフトウェアから構成されています。Open Sourceソフトウェアのインストールのみを決定できます。ただし、Sophos UTMの全機能を使用するためには、Enterprise Toolkitもインストールすることをお勧めします。

Enterを押して両方のソフトウェアパッケージをインストールするか、*いいえ*を選択してOpen Sourceソフトウェアのみをインストールします。

*インストール: パーティショニング*画面が表示されます。

13. **警告メッセージを確認してインストールを開始します。**

---

[1] たとえば、`255.255.255.0`というネットワークマスクを使用している場合、サブネットはアドレスの最初の3オクテットで定義されます。この場合は、`192.168.2`です。管理コンピュータのIPアドレスが`192.168.10.5`である場合、同じサブネット上にないため、ゲートウェイが必要になります。ゲートウェイルータは、`192.168.2`サブネット上にインタフェースが必要であり、管理コンピュータに連絡できなければなりません。この例では、ゲートウェイのIPアドレスは`192.168.2.1`とします。

警告は注意して読んでください。確認後、PCにすでに存在するすべてのデータが削除されます。

インストールをキャンセルしてリブートするには、*いいえ*を選択します。

> **警告 –** インストールプロセスを行うと、ハードディスクドライブ上のすべてのデータが削除されます。

ソフトウェアのインストールプロセスには最大2、3分かかる可能性があります。

*インストール完了*画面が表示されます。

14. **CD-ROMを取り出して、内部ネットワークに接続し、システムをリブートします。**
インストールプロセスが完了したら、ドライブからCD-ROMを取り出して、`eth0`ネットワークカードを内部ネットワークに接続します。内部ネットワークカード（`eth0`）を除き、ネットワークカードの順序は、通常PCI IDおよびカーネルドライバによって決定されます。ハードウェア構成を変更すると(特にネットワークカードを取り外した場合や追加した場合など)、ネットワードカード名の順序も変わる可能性があります。

    次に、インストール画面でEnterを押し、UTMをリブートします。ブートプロセス中に、内部ネットワークカードのIPアドレスが変わります。このとき、インストールルーチンコンソール（Alt+F1）に、「eth0にIPなし（No IP on eth0）」というメッセージが表示されます。

Sophos UTMのリブート後（ハードウェアによっては、このプロセスは数分かかります)、`eth0` インタフェースの IP アドレスを ping し、このアドレスが到達可能であることを確認します。接続できない場合、次のいずれかの問題が発生していないかチェックしてください。

- Sophos UTMのIPアドレスが誤っている。
- 管理者コンピュータのIPアドレスが正しくない。
- クライアントのデフォルトゲートウェイが正しくない。
- 正しくないネットワークカードにネットワークケーブルが接続されている。
- すべてのネットワークカードが同じハブに接続されている。

1.4 インストール手順

Sophos UTMインストールの2番目のステップはWebAdminで行います。これは、Webベースの管理インタフェースです。基本システム設定の前に、Sophos UTMをネットワークに統合する方法を計画しておく必要があります。どのような機能を提供するか（ブリッジモードと標準（ルーティング）モードの

どちらで運用するか、インタフェース間でデータパケットの流れをどのようにコントロールするかなど)を決定する必要があります。ただし、Sophos UTMは後でいつでも再設定できます。したがって、Sophos UTMをネットワークに統合する方法をまだ計画していない場合でも、すぐに基本設定に着手することも可能です。

1. **ブラウザを起動して、WebAdminを開きます。**
   Sophos UTMの URL(eth0 の IP アドレスなど)を参照します。上記の設定例との整合性を保つために、これは `https://192.168.2.100:4444` とします(プロトコルが HTTPS であり、ポート番号が 4444 であることに注意してください)。

   設定例と異なり、各Sophos UTMの出荷時は次のデフォルト設定になっています。

   - インタフェース: 内部ネットワークインタフェース(eth0)
   - **IP**アドレス: 192.168.0.1
   - ネットワークマスク: 255.255.255.0
   - デフォルトゲートウェイ: なし(none)

   任意のSophos UTMの WebAdmin にアクセスするには、代わりに次の URL を入力します。

   `https://192.168.0.1:4444`

   認証および暗号化された通信を提供するために、Sophos UTMには、自己署名済みのセキュリティ証明書が含まれています。この証明書は、WebAdmin への HTTPS 接続が確立するとWeb ブラウザに対して提示されます。証明書の有効期間を確認できない場合、ブラウザはセキュリティ警告を表示します。証明書に同意すると、最初のログインページが表示されます。

Welcome to WebAdmin

Basic system setup

Hostname:

Company or Organization Name:

City:

Country: :: Please select ::

admin account password:

Repeat password:

admin account email address:

These settings must be made before the system can be used. Please note that ALL fields must be filled in and the hostname must not contain special characters or spaces. After applying the settings, log into the system with username **admin** and the password you set below.

IMPORTANT--READ CAREFULLY BEFORE OPERATING THIS SOFTWARE

BY MARKING THE "ACCEPT"-CHECKBOX OR USING THIS SOFTWARE, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT, USE THE ESC KEY AND PROMPTLY RETURN THE SOFTWARE TOGETHER WITH ALL ACCOMPANYING ITEMS TO YOUR SUPPLIER FOR A FULL REFUND OF YOUR PAYMENT.

Astaro License Agreement
The installation and use of the Astaro Enterprise Toolkit as described in section I.is subject to the following terms and conditions which constitute a license agreement between Astaro GmbH & Co. KG, Germany ("Astaro") and the contracting individual or company ("User"). This agreement also applies to software updates, upgrades or any other additional components provided to the User by Astaro. All software components described in following section I. are hereafter collectively referred to as the Software.

Print EULA

I accept the license agreement

Perform basic system setup

図 **1** WebAdmin:初期ログインページ

2. **「基本システム設定」フォームに必要事項を入力します。**
   ここに表示されるテキストボックスに会社の情報を正確に入力します。さらに、管理者アカウントのパスワードと有効なメールアドレスを指定します。ライセンス条件に同意する場合は、*基本システム設定の実行*ボタンをクリックしてログインを続行します。基本システム設定の実行中、多数の証明書と認証局が作成されます。

   - **WebAdmin CA**:WebAdmin証明書が割り当てられたCA(*マネジメント* > *WebAdminの設定* > *HTTPS証明書*を参照)。
   - **VPNに署名するCA**:VPN接続に使用されるデジタル証明書に署名するCA(*サイト間VPN* > *認証管理* > *認証局を参照*)。
   - **WebAdmin証明書**:WebAdminのデジタル証明書(*サイト間VPN* > *証明書管理* > *証明書*を参照)。
   - **ローカルX.509証明書**:Sophos UTMVPN接続に使用される、のデジタル証明書(*サイト間VPN* > *証明書管理* > *証明書を参照*)。

ログインページが表示されます。(ただし、入力した値に基づいて証明書が変更されているため、一部のブラウザでは、さらにセキュリティ警告が表示される場合もあります。)
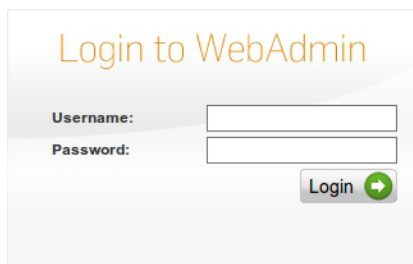
図**2** WebAdmin:通常のログインページ

3. **WebAdminにログインします。**
   *ユーザ名*フィールドに`admin`と入力し、前の画面で指定したパスワードを入力します。

   初期設定プロセスをガイドする設定ウィザードが表示されます。

   継続:ウィザードを使用する場合、このオプションを選択し、次に*次へ*をクリックします。ウィザードのステップに従い、Sophos UTMの基本設定を行います。

   バックアップのリストア:バックアップファイルがある場合、代わりにそのバックアップファイルをリストアするかを決めることができます。このオプションを選択し、*次へ*をクリックします。続行方法は、*バックアップリストア*セクションで説明されています。

   あるいは、(ウィザードの任意のステップで)*キャンセル*をクリックし、安全にウィザードを終了することもできます(Sophos UTMをWebAdminで直接設定したい場合など)。どの段階でも*終了*をクリックし、そこまでの設定を保存してウィザードを終了できます。

4. **ライセンスをインストールします。**
   購入したライセンス(テキストファイル)をアップロードするには、フォルダのアイコンをクリックします。*次へ*をクリックしてライセンスをインストールします。ライセンスを購入していない場合、*次へ*をクリックして、製品に組み込まれた30日間のトライアルライセンスを使用してください。Sophos UTMに搭載されたすべての機能が有効になります。

   注 **–** 選択されたラインセンスが特定のサブスクリプションを含まない場合、さらに先の手順の際、それぞれのページが無効化されます。

5. **内部ネットワークインタフェースを設定します。**

内部ネットワークインタフェース（*eth0*）に対して表示された設定を確認します。このインタフェースの設定は、ソフトウェアのインストール時に提供した情報に基づいています。さらに、チェックボックスにチェックを入れて、Sophos UTMが内部インタフェースで DHCP サーバーとして機能するように設定することができます。

> 注 – 内部インタフェースの IP アドレスを変更する場合、ウィザード終了後に新しい IP アドレスを使用して WebAdmin に接続し直す必要があります。

6. **外部インタフェースのアップリンクタイプを選択します。**
外部ネットワークカードで使用するアップリンク/インターネット接続の接続タイプを選択します。インタフェースのタイプとその設定は、どのような種類のインターネット接続を使用するかによって異なります。*次へ*をクリックします。

   Sophos UTMにアップリンクがないか、今すぐ設定したくない場合には、*インターネットアップリンクタイプ*入力ボックスを空欄のまま残します。インターネットアップリンクを設定すると、内部ネットワークからインターネットへの接続用に IP マスカレードが自動設定されます。

   *スタティックIP アドレスによる標準イーサネットインタフェース*を選択する場合、*デフォルトゲートウェイ*の指定はオプションです。テキストボックスを空欄のままにすると、インストール時のデフォルトゲートウェイ設定が維持されます。*次へ*をクリックして、残りの各ステップをスキップすることができます。スキップした設定は、後でWebAdminで設定・変更できます。

> 注 – ライセンスに次の機能の1つが許可されていない場合、関連機能は表示されません。

7. **基本的なファイアウォール設定を行います。**
ここで、インターネットで許可するサービスのタイプを選択できます。*次へ*をクリックして設定を確認します。

8. **高度な脅威防御設定を行います。**
ここで、複数のオペレーションシステムとデータベースに対する侵入防止およびコマンド&コントロール／ボットネット検出を設定できます。*次へ*をクリックして設定を確認します。

9. **Webプロテクション設定を行います。**
ここで、Webトラフィックに対してウイルスやスパイウェアのスキャンを行うかどうかを選択できます。さらに、特定のカテゴリに属する Web ページのブロックを選択できます。*次へ*をクリックして設定を確認します。

10. **Eメールプロテクション設定を行います。**

ここでは、最初のチェックボックスにチェックを入れて、POP3プロキシを有効にすることができます。ここでは、2つ目のチェックボックスにチェックを入れて、UTMをインバウンド SMTP リレーとして有効にすることができます。内部メールサーバーの IP アドレスを入力し、SMTP ドメインをルートに追加します。*次へ*をクリックして設定を確認します。

11. **ワイヤレスプロテクション設定を行います。**
    これにより、ワイヤレスプロテクションが有効になり、チェックボックスを選択することができます。ボックスで、ワイヤレスアクセスポイントとシステムの接続を許可するインターフェースを選択または追加します。インターフェースを追加するフォルダーアイコンをクリックするか、新規インターフェースを作成するために「+」アイコンをクリックします。別のワイヤレスネットワークパラメータを入力します。*次へ*をクリックして設定を確認します。

12. **詳細脅威適応型学習設定を行います。**
    Sophosのリサーチチームに匿名データを送信したい場合、この操作により、選択することができるようになります。このデータは、将来のバージョンの向上のため、またネットワークの可視性やアプリケーションコントロールライブラリの改良および拡張に使用されます。

13. **設定を確認します。**
    設定のサマリが表示されます。*終了*をクリックして確認するか、*戻る*をクリックして変更します。これらは後でWebAdminで変更することもできます。

    *終了*をクリックすると設定は保存され、ユーザはWebAdminのダッシュボードにリダイレクトされます。Sophos UTMここには、ユニットの最も重要なシステムステータス情報が表示されます。
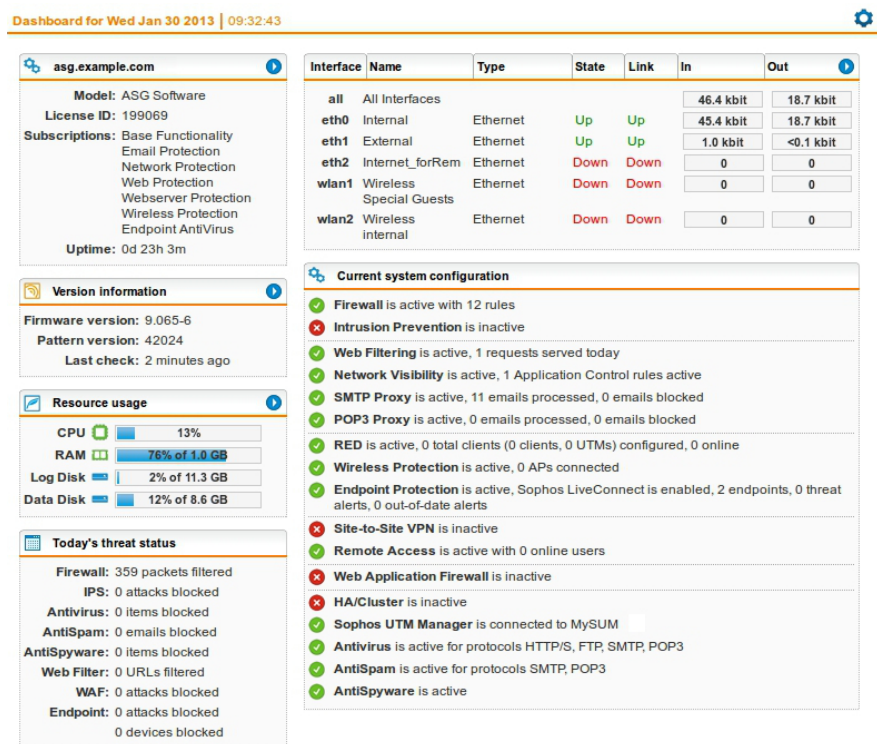
図3 WebAdmin:ダッシュボード

Sophos UTMこれらのステップの実行中に問題が発生した場合は、サプライヤのサポート部門にお問い合わせください。次のWebサイトでも詳細情報を提供しています。

- Sophos UTM サポートフォーラム
- Sophos Knowledgebase

1.5 バックアップリストア

WebAdmin設定ウィザード(*基本設定*のセクションを参照)を使用すると、基本設定プロセスをすべて実行する代わりに、既存のバックアップファイルをリストアすることができます。以下の手順に従ってください。

1. **設定ウィザードで*既存のバックアップファイルのリストア*を選択します。**
   設定ウィザードで*既存のバックアップファイルのリストア*を選択し、*次へ*をクリックします。

   アップロードページが表示されます。

2. **バックアップをアップロードします。**
   フォルダアイコンをクリックし、リストアするバックアップファイルを選択して、*アップロード開始*をクリックします。

3. **バックアップをリストアします。**
   *終了*をクリックしてバックアップをリストアします。

重要 – 後で設定ウィザードを使用することはできません。

バックアップのリストアが成功すると、ログインページにリダイレクトされます。

2 WebAdmin

WebAdminはWebベースの管理インタフェースで、ここではSophos UTMのあらゆる局面の設定を行うことができます。WebAdminはメニューとページで構成され、それらの多くには複数のタブが含まれています。画面左側のメニューには、Sophos UTMの機能が論理的に構成されています。*ネットワークプロテクション*などのメニュー項目を選択すると、それが拡大してサブメニューが表示されたり関連ページが開きます。メニュー項目の中には、関連ページがないものもあります。前に選択したメニューまたはサブメニュー項目のページは、そのまま表示されます。サブメニュー項目のいずれかを選択すると、それによって最初のタブの関連ページが開きます。

WebAdminを初めて開始する際、*設定ウィザード*が独自に表示されます。最も重要な設定のセットアップに関しては、取扱説明書に従います。

この管理ガイドの手順に従ってメニュー項目、サブメニュー項目、およびタブを指定すると、ページが開きます：例：*インタフェース&ルーティング* > *インタフェース* > *ハードウェア*タブ)。
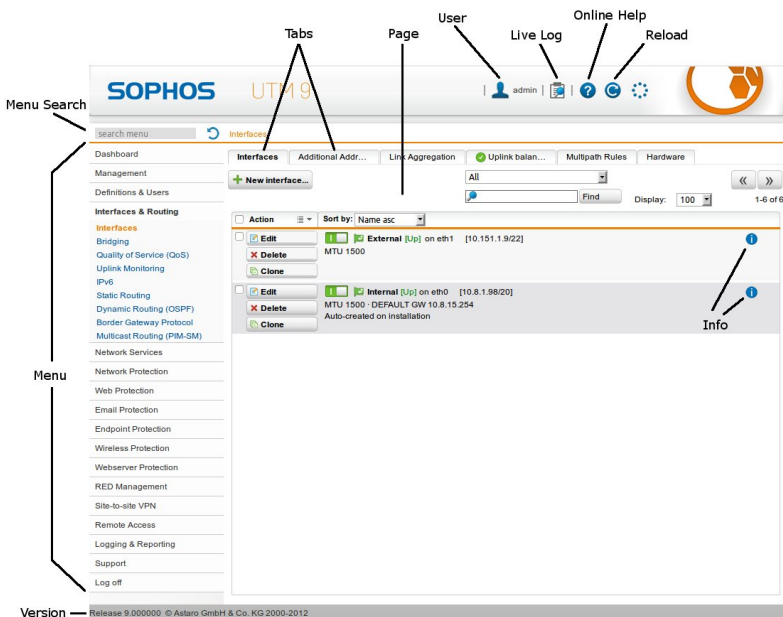
図4 WebAdmin：概要

2.1 WebAdmin メニュー

WebAdminメニューは、Sophos UTMのすべての設定オプションへのアクセスを提供します。したがって、特定パラメータの設定にコマンドラインインタフェースを使用する必要はありません。

- ダッシュボード: ダッシュボードは、Sophos UTMユニットの現在の操作状況をグラフィカルに表示します。
- マネジメント: 基本的なシステム設定、WebAdmin設定、Sophos UTMおよびユニットの設定に関するすべての設定を構成します。
- 定義とユーザ: Sophos UTMユニットで使用するネットワーク、サービス、時間帯定義、およびユーザアカウント、ユーザグループ、外部認証サービスを構成します。
- インタフェース& ルーティング: ネットワークインタフェースおよびルーティングオプションなどのシステム機能を設定します。
- ネットワークサービス: DNSやDHCPなどのネットワークサービスを設定します。
- ネットワークプロテクション: ファイアウォールルール、VoIP、侵入防御設定などの基本的なネットワークプロテクション機能を設定します。
- **Web**プロテクション: Sophos UTMユニットのWebフィルタおよびアプリケーションコントロール、ならびにFTPプロキシを設定します。
- **E**メールプロテクション: ユニットのSMTPおよびPOP3プロキシ、ならびにメールの暗号化を設定します。Sophos UTM
- エンドポイントプロテクション: 使用しているネットワークで、エンドポイントデバイスのプロテクションを設定、管理します。
- ワイヤレスプロテクション: ゲートウェイのワイヤレスアクセスポイントを設定します。
- **Web**サーバプロテクション: WebサーバをクロスサイトスクリプティングやSQLインジェクションなどの攻撃から防御します。
- **RED**マネジメント: REDアプライアンスを設定します。
- サイト間 **VPN**: サイト間VPN(バーチャルプライベートネットワーク)を設定します。
- リモートアクセス: Sophos UTMユニットへのリモートアクセスVPN接続を設定します。
- ログとレポート: Sophos UTMユニットの使用状況に関するログメッセージと統計を表示し、ログおよびレポーティングに関する設定を構成します。

- サポート: Sophos UTMユニットで利用できるサポートツールにアクセスします。
- ログオフ: ユーザインタフェースからログアウトします。

メニューの検索

メニュー上部に検索ボックスがあります。ここではキーワードについてメニューを検索し、特定のトピックに関するメニューを容易に検索できます。検索機能はメニュー名を検索しますが、非表示の索引付けされた別名やキーワードも検索できます。

検索ボックスに入力を開始するとすぐに、関連するメニュー項目のみが自動的に表示されます。検索ボックスはそのままにして、該当すると予想されるメニュー項目をクリックしてください。少なくなったメニュー項目はそのまま残り、その隣りのリセットボタンをクリックするまで検索結果が表示されます。

ヒント – キーボードショートカットCTRL+Yで検索ボックスにフォーカスすることができます。

2.2 ボタンバー

WebAdminの右上隅にあるボタンから、次の機能にアクセスできます。

- **ユーザ名/IP**: 現在ログインしているユーザと、WebAdminにアクセスしているIPアドレスを示します。現在他のユーザもログインしている場合は、他のユーザのデータも表示されます。
- ライブログを開く: このボタンをクリックすると、現在使用しているWebAdminメニューまたはタブに関連するライブログが開きます。メニューまたはタブを変更しなくても他のライブログを表示するには、ライブログボタンの上にカーソルを合わせます。数秒後に使用可能なすべてのライブログのリストが表示されるため、ここで表示するライブログを選択できます。この選択は、同じWebAdminメニューまたはタブを使用する限り、記憶されます。

  ヒント – 多くのWebAdminページに用意された *ライブログを開く* ボタンをクリックしてもライブログを開くことができます。

- オンラインヘルプ: すべてのメニュー、サブメニュー、タブにはオンラインヘルプ画面があり、WebAdminの現在ページのコントロールに関連するコンテキストに応じた情報や手順を提供します。

注 – オンラインヘルプはバージョンに基づいており、パターンによって更新されます。新しいファームウェアバージョンに更新したときに、オンラインヘルプの更新が利用できる場合は、オンラインヘルプも更新されます。

- リロード: すでに表示されているWebAdminページを再び要求する場合、必ず*リロード*ボタンをクリックしてください。

注 – ブラウザの「再読み込み」ボタンや「更新」ボタンは使用しないでください。これを行うと、WebAdminからログアウトすることになります。

2.3 リスト

WebAdminの多くのページにはリストがあります。各リストの左にあるボタンを使用すると、アイテムの編集、削除、または複製が可能です(詳しくは*ボタンとアイコン*セクションを参照してください)。リストにアイテムを追加するには、*新規...*ボタンをクリックします。ここで「...」は、作成中のオブジェクト(インタフェースなど)を示すプレースホルダです。ダイアログボックスが開き、新規オブジェクトのプロパティを定義することができます。
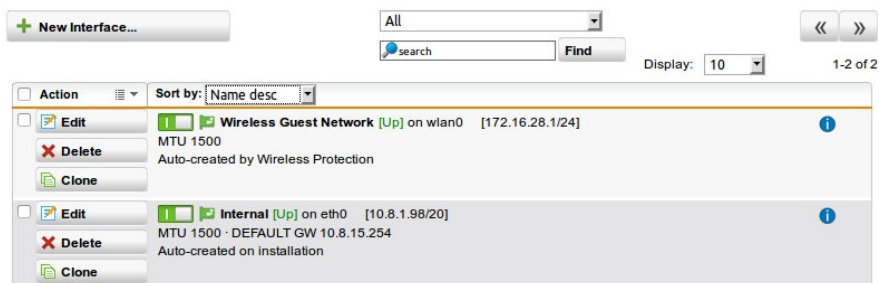
図 **5** WebAdmin:リストの例

一番上の最初のドロップダウンリストで、タイプまたはグループ別にすべてのアイテムをソートすることができます。上部にある2番目のフィールドを使用して、具体的なアイテムを検索することができます。検索文字列を入力し、*検索*をクリックします。

アイテムが11個以上含まれるリストは、複数ページに分割され、(>>)進むボタンと(<<)戻るボタンを使用して移動することができます。*表示*ドロップダウンリストで、ページ当たりのアイテム数を一時

的に変更することもできます。さらに、*マネジメント* > *WebAdmin設定* > *ユーザ設定*タブですべてのリストのデフォルト設定を変更することができます。

リストのヘッダには、機能があります。*ソート順*ドロップダウンリストからアイテムを選択すると、そのアイテムのリストが並べ替えられます。例えば、*Name asc*を選択するとオブジェクト名による昇順にリストが並べ替えられます。ヘッダの*アクション*フィールドには、選択しているリストオブジェクトに対して実行できるバッチオプションがあります。オブジェクトを選択するには、それぞれのチェックボックスを選択します。この選択は、複数ページにわたって維持されます。つまり、リストを数ページにわたって閲覧する間、既に選択したオブジェクトが選択された状態で維持されます。

ヒント – 情報アイコンをクリックすると、そのオブジェクトが使用されているすべての設定オプションが表示されます。

2.4 リストの検索

フィルタフィールドを使用すると、リストに表示される項目数を制限することができます。これにより、目的のオブジェクトを素早く探すことができます。

重要事項

- リストの検索では、通常複数のフィールドで検索式を検索します。たとえば、*ユーザとグループ*で検索を行うと、ユーザ名、実際の名前、コメント、最初のEメールアドレスが検索されます。一般的に、情報アイコンを使用して表示される情報を除いて、リストに表示されるすべてのテキストに検索が行われます。
- リストの検索では、大文字と小文字が区別されないため、大文字または小文字のどちらを入力しても同じ結果になります。検索結果には、一致した大文字と小文字のテキストが表示されます。大文字または小文字のテキストを限定して検索することはできません。
- リストの検索は、Perl正規表現構文に基づいています（しかし、大文字と小文字は区別されません）。テキストエディタなどでよく使用される * や ? などの単純なワイルドカード文字、AND や OR などの演算子をはじめとする検索式は、リスト検索では*機能しません*。

例

ここには、役立つ検索文字列をいくつか示します。

単純な文字列：指定した文字列を含むすべてのワードを検索します。たとえば、「inter」を指定すると、「Internet」、「interface」、「printer」が検索されます。

ワードの最初：検索文字列の最初に`\b`を付加します。たとえば、`\binter`を指定すると、「Internet」と「interface」が検索されますが、「printer」は検索されません。

ワードの最後：検索文字列の最後に`\b`を付加します。たとえば、`http\b`を指定すると、「http」が検索されますが、「https」は検索されません。

エントリの最初：検索文字列の最初に`^`を付加します。たとえば、`^inter`を指定すると、「Internet Uplink」が検索されますが、「Uplink Interfaces」は検索されません。

IPアドレス：IPアドレスを検索する場合は、ドットをバックスラッシュでエスケープする必要があります。たとえば、`192\.168`を指定すると、"192.168" が検索されます。IPアドレスをより一般的に検索するために、任意の数と一致する`\d`を使います。`\d+`を指定すると、行の複数の桁が一致します。たとえば、`\d+\.\d+\.\d+\.\d+`を指定すると、あらゆるIPv4アドレスが検索されます。

> 注 – より完全な検索文字列を指定すると、予想しない結果が得られたり、不正確な結論を導くことになるため、それよりは簡単で無難な検索文字列を使用して多くの検索結果を得ることをお勧めします。

正規表現の詳細とSophos UTMでの使用方法については、SophosKnowledgebaseを参照してください。

2.5 ダイアログボックス

ダイアログボックスとは、特定の情報の入力を求めるためにWebAdminが使用する特別なウィンドウです。この例では、*定義とユーザ* > *ユーザとグループ*メニュー内の新規グループを作成するためのダイアログボックスが示されています。

図 **6** WebAdmin:ダイアログボックスの例

各ダイアログボックスは、テキストボックス、チェックボックスなどの各種ウィジェットから構成されています。さらに、多くのダイアログボックスにはドラッグ＆ドロップ機能があり、*DND*と記された特別な背景で識別されます。このようなボックスが表示された場合、ボックスにオブジェクトをドラッグすることができます。オブジェクトをドラッグする元の場所となるオブジェクトリストを開くには、テキストボックスのすぐ横にあるフォルダアイコンをクリックします。これにより、設定オプションに応じて、使用可能なネットワーク、インタフェース、ユーザ/グループ、またはサービスのリストが開きます。緑色の「+」アイコンをクリックすると、ダイアログウィンドウが開き、新しい定義を作成することができます。特定の設定で不要なウィジェットは、グレーアウト表示されます。これらのウィジェットを編集できる場合もありますが、効果はありません。

注 – WebAdminには、*保存*ボタンと*適用*ボタンの両方が存在します。*保存*ボタンは、スタティックルートやネットワーク定義といったWebAdmin内のオブジェクトを作成または編集するときに使用します。常に、対応する*キャンセル*ボタンが用意されています。一方、*適用*ボタンは、バックエンドで設定を確認し、速やかに有効にするために使用します。

2.6 ボタンとアイコン

ここでは、WebAdminで使用されているボタンとアイコンの用途について説明します。

ボタン	機能アイコン
View	オブジェクトの詳細情報を示すダイアログウィンドウが表示されます。
Edit	オブジェクトのプロパティを編集するためのダイアログウィンドウが開きます。
Delete	オブジェクトを削除します。そのオブジェクトが他の箇所でまだ使用されている場合は、警告が表示されます。使用中のオブジェクトは削除できない場合があります。
Clone	同じ設定やプロパティで別のオブジェクトを作成するためのダイアログウィンドウが開きます。同じ設定を何度も繰り返し入力する必要なく、類似のオブジェクトを作成できます。

機能アイコン	意味
	情報: オブジェクトが使用されているすべての設定が表示されます。
	詳細: トピックに関する詳細情報がある、WebAdmin別のページにリンクします。
	トグルスイッチ: 機能を有効または無効にします。有効な場合は緑、無効な場合はグレー、有効化する前に設定が必要な場合はアンバーとなります。
	フォルダ: 2種類の機能があります。(1) 左側にあるオブジェクトリストを開く(下のセクションを参照)。ここで適切なオブジェクトを選択できます。(2) ファイルのアップロード用のダイアログウィンドウを開く。
	プラス + :必要なタイプの新しいオブジェクトを追加するためのダイアログウィンドウが開きます。
	アクション: アクションがあるドロップダウンメニューを開きます。アクションは、アイコンの場所によります。(1) リストヘッダにあるアイコン: アクション、例 *有効化*、*無効化*、*削除*、選択したリストオブジェクトへの適用。(2) テキストボックスにある場合、*インポート*/*エクスポート*を使用して、テキストをインポート/エクスポートできます。また、*空にする*を使って、コンテンツ全体を削除することもできます。一部の要素にリストを絞るためのフィルタフィールドも提供されています。フィルタでは大文字と小文字が区別されます。

機能アイコン	意味
	空にする: オブジェクトの前にある場合、現在の設定からオブジェクトを除去します。アクションメニューにある場合、ボックスからすべてのオブジェクトを除去します。ただし、このオブジェクトは削除されるわけではありません。
	インポート: 複数のアイテムまたは行を持つテキストをインポートするためのダイアログウィンドウが開きます。複数のアイテムを個別に入力するのではなく、まとめて追加することができます(たとえば、URL ブラックリストに大規模なブラックリストを追加する)。任意の場所からテキストをコピーし、CTRL+V で貼り付けます。
	エクスポート: 既存のアイテムをすべてエクスポートするためのダイアログウィンドウが開きます。アイテムを区切るための区切り文字として、新しい行、コロン、コンマのいずれかを選択できます。アイテムをテキストとしてエクスポートするには、エクスポートするテキストフィールドでテキスト全体を選択し、CTRL+C を押してコピーします。続いて、CTRL+V を使用してすべての共通アプリケーション(テキストエディタなど)にこれを貼り付けます。
	ソート: 2つの矢印を使用してリストの各要素を上下に動かし、並べ替えることができます。
« »	**進む/戻る:** 場所に応じて、長いリストのページを移動したり、変更や設定の履歴を前へ または後ろへ 移動することができます。
	PDF: 現在表示されているデータをPDF ファイルに保存してから、保存したファイルをダウンロードするためのダイアログウィンドウが開きます。
	CSV: 現在表示されているデータをCSV コンマ区切り値 ファイルに保存してから、保存したファイルをダウンロードするためのダイアログウィンドウが開きます。

2.7 オブジェクトリスト

オブジェクトリストとは、WebAdminの左側に一時的に表示されるドラッグ＆ドロップリストで、メインメニューをカバーします。
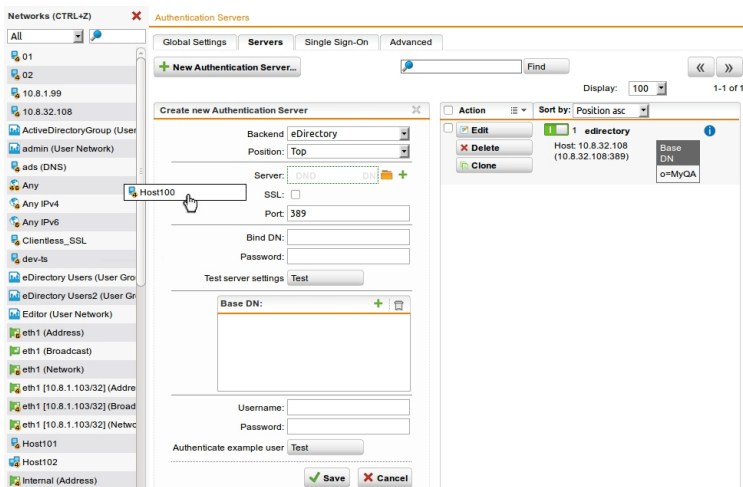
図 7 WebAdmin:オブジェクトリスト *ネットワーク*

オブジェクトリストは、フォルダアイコンをクリックすると自動的に開きます(上のセクションを参照)。あるいは、キーボードショートカットを使用して手動で開くこともできます(*マネジメント> WebAdmin設定 > ユーザプリファレンス*を参照)。

オブジェクトリストから、ユーザ/グループ、インタフェース、ネットワーク、サービスなどのWebAdminオブジェクトにすばやくアクセスし、設定時に選択することができます。オブジェクトを選択するには、現在の設定にオブジェクトをドラッグ&ドロップするだけです。

既存の各種オブジェクトタイプに従い、オブジェクトリストには5つのタイプがあります。「フォルダ」アイコンをクリックすると、現在の設定で必要なタイプが常に開きます。

3 ダッシュボード

ダッシュボードは、Sophos UTMの現在の操作状況をグラフィカルに表示します。特に、右上に表示されているダッシュボード設定アイコンを利用して、どのトピックセクションを表示するかを設定できます。設定についての詳細情報は、*ダッシュボード> ダッシュボード設定*で確認できます。

このダッシュボードにはデフォルトで、ユーザがいつWebAdminにログインしたのかを示す情報と次の情報が表示されます。

- 一般情報：ユニットのホスト名、モデル、ライセンスID、サブスクリプション、およびアップタイム。サブスクリプションの表示色は、有効期限が切れる30日前からオレンジ色に変わります。7日前から、また有効期限が切れると、サブスクリプションの表示色は赤になります。
- バージョン情報：現在インストールされているファームウェアとパターンバージョン、および利用可能な更新パッケージの情報。
- リソース使用状況：次のコンポーネントを含むシステムの現在の使用状況。
    - CPU 使用率（%）
    - RAM 使用率（%）表示される合計メモリは、オペレーティングシステムが使用できる部分であることに注意してください。32ビットシステムでは、一部がハードウェア用に予約されているため、必ずしも設置されている物理メモリの実際のサイズが表示されない場合もあります。
    - ログパーティションで消費されているハードディスクの容量（%）
    - ルートパーティションで消費されているハードディスクの容量（%）
    - UPS（無停電電源装置）モジュールがある場合はその状況
- 今日の脅威ステータス：深夜以降に検出された関連するセキュリティ脅威のカウンタ：
    - ログが有効になっているドロップされたデータパケットと拒否されたデータパケットの合計
    - 侵入がブロックされた回数の合計
    - ブロックされたウイルスの合計（全プロキシ）
    - ブロックされたスパムメッセージの合計（SMTP/POP3）
    - ブロックされたスパイウェアの合計（全プロキシ）
    - ブロックされたURLの合計（HTTP/S）

- ブロックされたWebサーバ攻撃の合計(WAF)
  - ブロックされたエンドポイント攻撃およびブロックされたデバイスの合計
- インタフェース: 設定されているネットワークインタフェースカードの名前とステータス。さらに、受信トラフィックと送信トラフィックの両方に対する過去75秒間の平均ビットレートに関する情報も表示されます。表示される値は、15秒間隔で収集されるサンプルに基づく平均ビットレートから取得されます。インタフェースのトラフィックアイコンをクリックすると、フローモニタが新しいウィンドウで開きます。フローモニタには、過去10分間のトラフィックが表示され、短い間隔で自動更新されます。フローモニタについて詳しくは、*フローモニタ*を参照してください。
- 高度な脅威防御 **(ATP)**: 高度な脅威防御のステータス。表示は、高度な脅威防御が有効であるかどうか、および感染したホストのカウンタを示しています。
- 現在のシステム設定: 最も関連するセキュリティ機能が有効であるか無効であるかを示します。エントリの1つをクリックすると、それぞれの設定と共にWebAdminページが開きます:
  - ファイアウォール: アクティブファイアウォールルールの合計に関する情報。
  - **IPS**: 侵入防御システム(IPS)は、シグニチャに基づくIPSルールセットを利用して攻撃を認識します。
  - **Web**フィルタリング: HTTP/Sプロトコル用のアプリケーションレベルのゲートウェイ。サービスの使用が許可されているネットワークに対し、豊富なWebフィルタ技術を提供します。
  - ネットワーク可視化: **Sophos'** レイヤ**7**アプリケーションコントロールを使用すると、ネットワークトラフィックを分類およびコントロールできます。
  - **SMTP**プロキシ: SMTP(*簡易メール転送プロトコル*)を使用したメッセージ送信用のアプリケーションレベルのゲートウェイ。
  - **POP3**プロキシ: POP3(*Post Office Protocol 3*)を使用したメッセージ送信用のアプリケーションレベルのゲートウェイ。
  - **RED**: 支社のセキュリティのためのリモートイーサネットデバイス(RED)アプライアンスの設定。
  - ワイヤレスプロテクション: ワイヤレスネットワークおよびアクセスポイントの設定。
  - エンドポイントプロテクション: ネットワークにおけるエンドポイントデバイスの管理。接続されているエンドポイントおよびアラートの数を表示します。
  - サイト間 **VPN**: サイト間VPNシナリオの設定。
  - リモートアクセス: ロードウォリアVPNシナリオの設定。

- **WAF**:Webサーバをクロスサイトスクリプティングや SQL インジェクションなどの攻撃から防御するためのアプリケーションレベルのゲートウェイ。
- **HA/**クラスタ:冗長化(HA)フェイルオーバおよびクラスタリング。つまり、処理集約型のタスク(コンテンツフィルタ、ウイルススキャン、侵入検知、復号化など)を複数のクラスタノードに均一に分散します。
- **Sophos UTM Manager**: Sophos UTM集中管理ツールSophos UTM Manager(SUM)によるアプライアンスの管理。
- **Sophos**モバイル制御:コンテンツ、アプリケーション、Eメールを制御するためのモバイルデバイスの管理。
- ウイルス対策:ウイルス、ワーム、その他のマルウェアなどの有害で危険なコンテンツを伝送するWebトラフィックからネットワークを保護します。
- スパム対策:未承諾のスパムメールを検知し、既知の(または疑わしい)スパム発信者からのスパム送信を特定します。
- スパイウェア対策:シグニチャデータベースとスパイウェアフィルタリング技術が定期的に更新される2種類のウイルススキャンエンジンを使用して、スパイウェア感染を防止します。受信トラフィックと送信トラフィックの両方を保護します。

3.1 ダッシュボード設定

ダッシュボードでは、いくつかの設定を変更できます。ダッシュボード右上のダッシュボード設定アイコンをクリックすると*ダッシュボード設定の編集*ダイアログウィンドウが開きます。

ダッシュボードの更新:デフォルトで、ダッシュボードは5秒間隔で更新されます。更新間隔は*無し*～*毎分*の間で設定できます。

左の列 – 右の列:ダッシュボードは、各トピックに関する情報を示すいくつかのトピックセクションに分かれています。*左の列*および*右の列*の 2つのボックスを使用すると、これらのトピックセクションの配置を変えたり、表示に追加したり表示から削除することができます。これらの設定がその後ダッシュボードに反映されます。列のトピックセクションを並べ替えるには、矢印アイコンを使用します。特定のトピックセクションを表示に追加したり表示から削除するには、チェックボックスにチェックを入れるか、外します。

デフォルトで表示されるトピックセクションについては、「ダッシュボード」の章を参照してください。追加のトピックセクションも表示することができ、ここでそれについて説明します。

- **Web**プロテクション: 上位アプリ: 最もよく使用されているアプリケーションの概要。このセクションで、アプリケーションの上にカーソルを移動させると、追加の機能を提供するアイコンが1つか2つ表示されます。
  - *ブロック*アイコンをクリックすると、現時点から該当アプリケーションがブロックされます。これにより、*アプリケーション制御ルール*ページにルールが作成されます。このオプションは、Sophos UTMの正常なオペレーションに必要なアプリケーションに対しては利用できません。たとえば、WebAdminトラフィックはブロックできません。これをブロックすると、ユーザ自身がWebAdminからシャットアウトされてしまいます。未分類のトラフィックもブロックできません。
  - *シェーピング*アイコンをクリックすると、それぞれのアプリケーションのトライフィックシェーピングが有効になります。ダイアログウィンドウが開き、ルール設定を定義するよう要求されます。完了したら*保存*をクリックします。これにより、*および帯域幅プール*ページの両方にルールが作成されます。シェーピングはインタフェース単位で機能するため、*すべてのインタフェース*フローモニタを閲覧している際はトラフィックシェーピングを利用できません。
  - *帯域幅調整*アイコンをクリックすると、それぞれのアプリケーションのトライフィック帯域幅調整が有効になります。ダイアログウィンドウが開き、ルール設定を定義するよう要求されます。完了したら*保存*をクリックします。これにより、*トラフィックセレクタ*および*ダウンロード帯域幅調整*ページにルールが作成されます。ダウンロード帯域幅調整はインタフェース単位で機能するため、*すべてのインタフェース*フローモニタを閲覧している際はダウンロード帯域幅調整を利用できません。
- **Web**プロテクション: 時間別の上位サイト: 最もよく閲覧されたドメインの時間別の概要。
- **Web**プロテクション: トラフィック別の上位サイト: 最もよく閲覧されたドメインのトラフィック別の概要。
- ログ: ディスクのSophos UTM残容量、フィルアップレート(使用量増加速度)の情報を含むユニットのログパーティションのステータス。
- ニュースフィード: Sophosおよびその製品に関するニュース。
- グラフ: 同時接続 : 同時接続の総数に関する日々の統計およびヒストグラム。
- グラフ: ログパーティションステータス: ログパーティションの使用状況に関する過去4週間の統計およびヒストグラム。
- グラフ: **CPU**の使用状況 : 現在のプロセッサ使用状況(%)に関する日々の統計およびヒストグラム。
- グラフ: メモリ/スワップの使用状況 : メモリおよびスワップ使用状況(%)に関する日々の統計およびヒストグラム。

- *グラフ: パーティション使用状況*:選択したパーティションの使用状況(%)に関する日々の統計およびヒストグラム。

ダッシュボードでの自動グループ化の有効化:ダッシュボード上にコンパクトに情報を表示するにはこのオプションを選択します。このオプションは、左の列の*Web プロテクション*の選択項目と、右の列の*グラフ*の選択項目のみに影響を及ぼします。これを選択すると、各情報要素がダッシュボード上のタブとして重なって表示されます。選択を解除すると、情報要素が左右に並んで表示されます。

*保存*をクリックして設定を保存します。

3.2 フローモニター

Sophos UTMのフローモニタは、現在UTMのインタフェースを通過しているネットワークトラフィックに関する情報を素早く確認するためのアプリケーションです。ダッシュボードの右上でいずれかのインタフェースをクリックすることにより簡単にアクセスできます。*すべてのインタフェース*をクリックすると、すべてのアクティブなインタフェースについて蓄積されたトラフィックがフローモニタに表示されます。単一のインタフェースをクリックすると、そのインタフェースのトラフィックのみがフローモニタに表示されます。

注 – フローモニタは新しいブラウザウィンドウで開きます。このウィンドウはポップアップブロッカによってブロックされる可能性があるため、WebAdminに対してポップアップブロッカを無効にすることをお勧めします。

フローモニタには、グラフとテーブルという2種類のビューがあります。それぞれについては後述します。ビューは5秒間隔で更新されます。更新を停止するには*一時停止*ボタンをクリックします。*続行*をクリックして更新を再開すると、フローモニタが最新のトラフィック情報に更新します。

テーブルビュー

フローモニタのテーブルには、過去5秒間のネットワークトラフィックに関する情報が表示されます。

#:トラフィックは、現在の帯域幅使用状況に基づいてランク付けされます。

Application(*アプリケーション*):利用可能な場合、ネットワークトラフィックのプロトコルまたは名前。未分類のトラフィックは、システムにとって不明な種類のトラフィックです。アプリケーションをクリックすると、ウィンドウにサーバ、使用ポート、サーバ接続ごとの帯域幅の使用状況、合計トラフィックの情報が表示されます。

Client(クライアント**):** アプリケーションを使用しているクライアント接続数。クライアントをクリックすると、ウィンドウにクライアントのIPアドレス、クライアント接続ごとに使用される帯域幅、合計トラフィックの情報が表示されます。未分類のトラフィックの場合は、テーブル内のクライアント数が追加情報ウィンドウに表示されるクライアント数よりも多くなる可能性があります。これは「未分類」に複数のアプリケーションが含まれるためです。したがって、情報ウィンドウのクライアント数が1つでもテーブルには3つのクライアントが存在する場合があります。これは、1つのクライアントが3種類の未分類のアプリケーションに接続していることが考えられます。

Bandwidth Usage Now(現在の帯域幅使用状況**):** 過去5秒間の帯域幅使用状況。帯域幅をクリックすると、ウィンドウにアプリケーション接続のダウンロード速度とアップロード速度の情報が表示されます。

Total Traffic(合計トラフィック**):** 接続の「ライフタイム」中に生成されたネットワークトラフィックの合計数。例1:ダウンロードが、過去のある時点で開始され、まだ継続中です。ダウンロード開始時点から、期間中に生成されたトラフィック全体が表示されます。例2:複数のクライアントがFacebookを使用しています。いずれか1つのクライアントが接続をオープンにしている限り、すべてのクライアントによってこれまでに生成されたトラフィックがすべて蓄積されて合計トラフィックに表示されます。

合計トラフィックをクリックすると、ウィンドウにアプリケーション接続の総合ダウンロード速度とアップロード速度の情報が表示されます。

Actions(*アクション***):** アプリケーションの種類に応じて、利用可能なアクションがあります(未分類のトラフィックを除く)。

- ブロック:*Block*ボタンをクリックすると、現時点から該当アプリケーションがブロックされます。これにより、*アプリケーション制御ルール*ページにルールが作成されます。このオプションは、Sophos UTMの正常なオペレーションに必要なアプリケーションに対しては利用できません。たとえば、WebAdminトラフィックはブロックできません。これをブロックすると、ユーザ自身がWebAdminからシャットアウトされてしまいます。未分類のトラフィックもブロックできません。
- トラフィックシェーピング:シェーピング(*Shape*)ボタンをクリックすると、それぞれのアプリケーションのトライフィックシェーピングが有効になります。ダイアログウィンドウが開き、ルール設定を定義するよう要求されます。完了したら*保存*をクリックします。これにより、*および帯域幅プール*ページの両方にルールが作成されます。シェーピングはインタフェース単位で機能するため、*すべてのインタフェース*フローモニタを閲覧している際はトラフィックシェーピングを利用できません。
- ダウンロード帯域幅調整:*Throttle*ボタンをクリックすると、当該アプリケーションのダウンロード帯域幅の調整が有効になります。ダイアログウィンドウが開き、ルール設定を定義するよう要求されます。完了したら*保存*をクリックします。これにより、*トラフィックセレクタ*および*ダウ*

*ンロード帯域幅調整*ページにルールが作成されます。ダウンロード帯域幅調整はインタフェース単位で機能するため、*すべてのインタフェース*フローモニタを閲覧している際はダウンロード帯域幅調整を利用できません。

グラフビュー

フローモニタのグラフには、過去10分間のネットワークトラフィックが表示されます。横軸は時間を、縦軸はスループットにスケールを動的に適用したときのトラフィック量を示します。

グラフビューの下部には、インタフェースを通過するトラフィックの種類を示す凡例が表示されます。トラフィックは種類ごとに色分けされるため、グラフ内で簡単に見分けることができます。

注 – ネットワーク可視化を有効にした場合（*Webプロテクション* > *アプリケーション制御* > *ネットワーク可視化*の章を参照）、フローモニタはトラフィックについてより差別化された情報を表示します。

マウスのカーソルをグラフ上に置くと、大きなドット（点）が表示され、グラフのその部分の詳細な情報が表示されます。このドットは、グラフの線に沿って移動します。マウスのカーソルを移動すると、ドットもそれに従って移動します。グラフに何本かの線がある場合、ドットはマウスカーソルの移動に従って線の間を移動します。さらに、ドットの色は、それが表示している情報がどの線に関連するかによって変わるため、線が互いに近接している場合に役立ちます。ドットは、ある時点でのトラフィックの種類とサイズに関する情報を示します。

4 マネジメント

この章では、基本システム設定や、Sophos UTMなどのWebベース管理インタフェースの設定を、定義する方法を説明します。*概要*ページには、加えられた可能性のある変更を含め、最近のWebAdminセッションの統計が表示されます。変更の詳細を確認するには、*変更ログ*列の*表示*ボタンをクリックします。

*状態*列には、前回のWebAdminセッションの終了時間が表示されます。

注 – WebAdminセッションを終了するには、*ログオフ*メニューをクリックします。*ログオフ*メニューをクリックしないでブラウザを閉じた場合、セッションは*マネジメント* > *WebAdmin設定* > *詳細*タブで定義されている期間の後にタイムアウトします。

この章には次のトピックが含まれます。

4.1 システム設定

システム設定メニューで、UTMの基本設定を設定できます。ホスト名、日付、時刻設定のほか、ウイルス対策エンジンのスキャン設定または高度な脅威防御オプションを設定できます。また、設定またはパスワードのリセットや、SSHシェルアクセス設定も行えます。

4.1.1 組織

以下の組織情報を入力します(インストールウィザードにより行われていない場合)。

- 組織名 : 組織の名前です。
- 市 : 組織の所在地です。
- 国 : 組織が所在する国です。
- 管理者のEメールアドレス: Sophos UTMの技術サポートを担当する人物またはグループに連絡するためのEメールアドレスです。

このデータは、IPsec、Eメール暗号化、およびWebAdminの証明書でも使用されます。

4.1.2 ホスト名

完全修飾ドメイン名(FQDN)として、UTMのホスト名を入力します。完全修飾ドメイン名とは、DNSツリー階層でのノードの絶対位置を指定する明瞭なドメイン名です(`utm.example.com`など)。ホスト名には英数字、ドット、およびハイフンを使用できます。ホスト名の末尾には`com`、`org`、`de`などの特殊な識別子を使用する必要があります。ホスト名は、通知メッセージでUTMを識別するために使用されます。また、Webフィルタから送信されたステータスメッセージにも表示されます。お客様のドメインのDNSゾーンにホスト名を登録する必要はありません。

4.1.3 日付と時刻

UTMでは、日付と時刻を常に正しく設定しておく必要があります。これは、ロギングおよびレポーティングシステムから正しい情報を取得したり、インターネット上の他のコンピュータとの相互運用性を保証するために必要です。

通常は、日付と時刻を手動で設定する必要はありません。デフォルトで、パブリックのインターネットサーバとの自動同期が有効化されています(*インターネットサーバと時間を同期*のセクションを参照)。

まれではありますが、タイムサーバとの同期を無効にする必要がある場合、時刻と日付を手動で変更することができます。ただし、これを行う場合は、以下の警告に注意してください。

- システム時間を標準時間からサマータイムに(あるいはその逆に)変更しないでください。この変更は、タイムサーバとの自動同期を無効にした場合でも、タイムゾーンの設定によって自動的に行われます。
- タイムサーバとの同期が有効になっている場合は、日付または時刻を手動で変更しないでください。多くの場合、自動同期により、手動で行った変更がすぐに取り消されます。日付または時刻を手動で設定する必要がある場合、最初に*NTPサーバ*ボックス(下の*インターネットサーバと時間を同期*セクション)からすべてのサーバを削除し、*適用*をクリックしてください。
- システム時間を手動で変更してから、変更が成功したことを通知する緑色の確認メッセージが表示されるまで待機します。次に、システムをリブートします(*マネジメント* > *シャットダウン/リスタート*)。多くのサービスでは、時間は連続的に変化し、急に変化する訳ではないという事実に依存しているため、これが推奨されます。時間に飛びがあると、様々なサービスの誤作動につながる可能性があります。このアドバイスは、あらゆる種類のコンピュータシステムに共通して該当します。
- まれに、システム時間を変更すると、WebAdminセッションが強制終了される可能性があります。これが発生した場合、ログインし直して、時刻が正しく設定されていることを確認し、後でシステムを再起動してください。

UTMこれは、アカウンティングとレポートデータをさらに処理する必要がある場合やデータの精度が重要な場合には、特に言えることです。

これは、レポートデータをさらに処理する必要がある場合やデータの精度が重要な場合には、特に言えることです。

- 時刻を早める
  - 時刻に基づくレポートの場合、スキップされた時間のデータがなくなります。ほとんどのグラフでは、この期間は、最近記録された値が直線で表示されます。
  - アカウンティングレポートでは、この期間は、すべての変数が0で表示されます。
- 時刻を戻す
  - 時刻に基づくレポートには、該当する期間のログデータがすでに存在します。
  - ほとんどの図は、この期間に記録された値を圧縮して表示します。
  - ダッシュボードで表示される最後のパターンチェックからの経過時間は、たとえ最後のチェックがほんの数分前に行われた場合であっても、値について「なし」と表示します。

- UTM上で自動的に作成された証明書は、それらの有効期間の開始日付が将来になっている場合は無効になります。
- アカウンティングレポートは将来の時刻から記録された値を保持します。再度リセットの時刻になると、アカウンティングデータは再度通常どおりに記述されます。

こうした欠点があるため、システム時間はシステムのセットアップ時に一度だけ設定し、その後は少し調整するだけにするべきです。これは、レポートデータをさらに処理する必要がある場合やデータの精度が重要な場合には、特に言えることです。

日付と時刻の設定

システム時間を手動で設定するには、日付と時刻をそれぞれのドロップダウンリストから選択します。設定を保存するには*適用*をクリックします。

タイムゾーンの設定

システムのタイムゾーンを変更するには、ドロップダウンリストから地域またはタイムゾーンを選択します。設定を保存するには*適用*をクリックします。

タイムゾーンを変更してもシステム時間は変更されず、影響があるのは、ロギングデータやレポーティングデータなどの出力における時間の表示のみです。サービスの妨げとなることはなくても、すべてのサービスが新しい時間設定を確実に使用するように後でリブートすることを強く推奨いたします。

インターネットサーバとの時刻同期

タイムサーバを使用してシステム時刻の同期をとるには、1台以上のNTPサーバを選択します。設定を終了したら*適用*をクリックします。

NTPサーバ：デフォルトでは*NTP Server Pool*が選択されています。このネットワーク定義は*pool.ntp.org*プロジェクトのパブリックタイムサーバの大きな仮想クラスタにリンクしています。インターネットサービスプロバイダが顧客用にNTP サーバを運用しており、これらのサーバへのアクセス権がある場合、*NTP Server Pool*を削除してプロバイダのサーバを使用することが推奨されます。独自のサーバまたはプロバイダのサーバを選択する場合、複数のサーバを使用すると、精度や信頼性が向上します。3つの独立したサーバを使用すれば、常に十分です。それ以上のサーバを追加しても、さらなる改良はほとんど期待できず、サーバの負荷が増加します。*NTP Server Pool*と独自またはプロバイダのサーバの両方を使用しても、精度や信頼性は向上しないため、使用は推奨されません。

ヒント – クライアントコンピュータをこれらのNTP サーバと接続可能にするには、*ネットワークサービス > NTP*ページの許可ネットワークに追加します。

テスト構成サーバ：デバイスから選択されたNTPサーバへの接続を確立できることと、NTPサーバが使用可能な時刻データを返すことをテストする際は、このボタンをクリックします。これで、お使いのシステムとサーバ間の時間のオフセットを測定します。お使いのシステムが正しく設定されており、一定時間にわたって安定した状態で動作している場合は、オフセットは一般的に1秒未満になります。

通常、NTPを有効化したり他のサーバを追加した直後は、オフセットがこれより長くなります。時間の飛びを防ぐために、NTPはゆっくりとシステム時間をずらします。やがて、システム時間は時間の飛びなく補正されます。このような状況が発生した場合は、しばらく待機してください。特に、このような場合には、システムを再起動*しないでください*。その代わりに、約1時間後に再びチェックしてください。オフセットが減少すると、すべてが正しく機能するようになります。

4.1.4 シェルアクセス

セキュアシェル（SSH）はコマンドラインアクセスモードであり、主にUTMへのリモートシェルアクセスを取得するために使用されます。これは通常、より深いレベルのメンテナンスやトラブルシューティングに使用されます。このシェルにアクセスするには、SSHクライアントが必要です。SSHクライアントは一般的に、ほとんどのLinuxディストリビューションに装備されています。Windowsの場合、無料のSSHクライアントをダウンロード可能です。例：PuTTY（www.putty.org）またはDameWare（www.dameware.com）。

許可ネットワーク

*許可ネットワーク*コントロールを使用して、この機能へのアクセスを特定ネットワークのみに制限します。ここにリストされたネットワークは、SSHサービスに接続できます。

認証

このセクションで、SSHアクセスの認証方法とアクセスの厳格さを定義できます。以下の認証方法を利用できます。

- パスワード（デフォルト）
- 公開鍵
- パスワードと公開鍵

これらのオプションを利用するには、対応するチェックボックスを選択します。*公開鍵認証*を使用するには、公開鍵での認証を許可された各ユーザについて、それぞれの公開鍵を*ログインユーザに承認された鍵*フィールドにアップロードする必要があります。

rootログインの許可：rootユーザに対してSSHアクセスを許可できます。このオプションを有効にするとセキュリティリスクが高くなるため、デフォルトでは無効になっています。このオプションを有効

にすると、ルートユーザは公開鍵を介してログインできます。*root用の公開鍵*フィールドにrootユーザの公開鍵をアップロードします。

注 - Sophos Knowledgebase内でのSSH鍵作成についての詳細は、*PuTTYを使用する*、*Linuxベースのシステム上のSSH鍵*の作成の項でご確認ください。

設定を保存するには*適用*をクリックします。

シェル ユーザ パスワード

デフォルトのシェルアカウント`root`(ルート)および`loginuser`(ログインユーザ)用のパスワードを入力します。これら2つのアカウントのいずれか一方のパスワードのみを変更するには、他方のアカウントの入力ボックスを空白のままにします。

注 –SSHシェルアクセスを有効にするには、最初にパスワードを設定する必要があります。さらに、*定義とユーザ* > *認証サービス* > *詳細*タブで設定したパスワードの複雑さの設定に準拠したパスワードのみを指定できます。つまり、複雑なパスワードを有効にした場合は、シェルユーザのパスワードも同じ要件を満たすことが必要になります。

SSH経由でのUTMへのアクセス

SSH経由でUTMへアクセスするには、通常のSSHユーティリティプログラム(PuTTYなど)を利用して、SSHポート(デフォルトではTCP 22)経由で接続します。

ログインユーザとして、

- `loginuser`およびSSHで上記で設定された関連パスワードをプロンプトして、ログイン可能です。または、
- ログインユーザとしてログイン後に、`su -` とタイプし上記で設定された関連パスワードを入力してルート可能です。

注 - *ルート*を利用して行った変更により、サポートが無効となります。代わりに、設定変更にはWebAdminを使用します。

SSHデーモンリスニングポート

このオプションで、SSHに使用するTCPポートを変更できます。デフォルトでは、標準SSHポートの`22`が設定されています。ポートを変更するには、`1024`～`65535`の適切な値を*ポート番号*ボックスに入力し、*適用*をクリックします。

4.1.5 スキャン設定

親プロキシ

親プロキシは、多くの場合、政府承認のプロキシサーバを通してインターネットアクセスをルーティングする必要のある国で必要とされます。親プロキシの使用がセキュリティポリシで求められている場合、ここでホスト定義とポートを選択して親プロキシを設定できます。

親プロキシを使用:

1. 親プロキシの使用を有効にするには、チェックボックスにチェックを入れます。
2. ホストを選択または追加します。
3. **プロキシのポートを入力します。**
   定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。
4. ***適用*をクリックします。**
   設定が保存されます。

プロキシ認証を使用:親プロキシで認証が必要な場合、ここでユーザ名とパスワードを入力します。

ウイルス対策エンジン設定

WebAdminを通してすべてのシングルスキャン設定に使用するウイルス対策エンジンを選択します。デュアルスキャン設定では、両方のウイルス対策エンジンが使用されます。デュアルスキャンは、ベーシックガードサブスクリプションでは使用できません。設定を保存するには*適用*をクリックします。

高度な脅威防御オプション

保護を強化するため分析オプションに対し、*疑わしいファイルは分析のためSophosLabs(ソフォスラボ)へ送信*を選択します。SophosLabsは、疑わしいマルウェアのふるまいを自動的に観察、分析するクラウドベースのサンドボックスが特徴です。これにより、使用しているUTMに対し、保護の更新の迅速な配信を確保するのに役立ちます。この機能を無効にした場合、防御の応答時間が長くなる可能性があります。

すべての送信に関し、セキュアなチャネルで送信され、SophosLabs情報セキュリティポリシに従って取り扱われます。

4.1.6 設定 または パスワードのリセット

*設定 または パスワードのリセット*タブのオプションで、シェルユーザのパスワードを削除できます。さらに、工場リセットを実行して、UTMのシステムIDをリセットすることができます。

システムパスワードのリセット

*システムパスワードを今すぐリセット*機能を実行すると、以下のユーザのパスワードがリセットされます。

- root ユーザ（シェルユーザ）
- loginuser（シェルユーザ）
- admin（事前に定義されている管理者アカウント）

さらに、システムを停止するには、*後でシステムをシャットダウン*オプションを選択します。

セキュリティに関する注記 – 次にiView Setupに接続する人に対して、*admin パスワード設定*ダイアログウインドウが表示されます。したがって、パスワードをリセットしたら、すぐにログアウトし、ブラウザでそのページをリロード（再読み込み）して、新しいadminパスワードを設定してください。

また、*マネジメント* > *システム設定* > *シェルアクセス*タブで新しいシェルパスワードを設定しない限り、シェルアクセスは実行できなくなります。

出荷時設定に初期化する

*今すぐ工場リセット*機能は、デバイスを工場出荷時のデフォルト設定にリセットします。以下のデータが削除されます。

- システム設定
- Webフィルタキャッシュ
- ログおよびレポーティングデータ
- データベース
- 更新パッケージ
- ライセンス
- パスワード
- HAステータス

ただし、Sophos UTMソフトウェアのバージョン番号はそのままです。つまり、インストールされたすべてのファームウェアおよびパターンの更新が維持されるということです。

注 – Sophos UTMは、出荷時設定への初期化が開始するとシャットダウンします。

UTM ID リセット

*UTM IDをすぐにリセット*機能では、UTMのシステムID を新しい、ランダム値にリセットします。これは、たとえばエンドポイントプロテクションを使用する場合に関連します。エンドポイントプロテクションを使用するすべてのUTMは、一意のシステムIDによってSophosLiveConnectで自身を識別します。たとえば、エンドポイントプロテクションを使用して仮想UTMを複製し、複製でもそUTMれを使用したい場合は、以後、新しいシステムIDで識別できるように、複製されたのシステムID をリセットする必要があります。リセット中、オンにすると、エンドポイントプロテクションはオフになります。

注 – エンドポイントは、UTMシステムIDを使用して、UTMに接続されます。UTMシステムID をリセットし、他に古いUTMIDでリスンしているUTMがなければ、エンドポイントを再インストールする必要があります。

注 – UTMがSophosUTMManagerに接続されていて、そのUTMシステムIDをリセットすると、UTMは新しいデバイスとして接続されます。必要であれば、2つのデバイスを管理できます。

4.2 WebAdmin設定

マネジメント > *WebAdmin設定*の下にあるタブで、アクセスコントロール、TCPポート、HTTPS証明書、ユーザ設定、およびWebAdminの言語といったWebAdminの基本設定を構成できます。

4.2.1 一般

WebAdmin設定 > *一般*タブで、WebAdmin言語と基本アクセス設定を構成できます。

WebAdmin 言語

WebAdminの言語を選択します。選択した言語も、一部のWebAdmin出力で使用できます。例、メール通知、実行レポート。例、実行レポート。これはグローバル設定で、すべてのユーザに適用されます。設定を保存するには*適用*をクリックします。

言語を変更した場合、ブラウザのキャッシュを空にして、すべてのテキストが正しい言語で表示されていることを確認する必要があります。

WebAdminアクセス設定

ここで、WebAdminへのアクセスが許可されるユーザやネットワークを設定できます。

許可する管理者: Sophos UTMは同時に複数の管理者によって管理できます。*許可された管理者*ボックスで、WebAdminインタフェースへの無制限の読み取りおよび書き込みアクセスを持つユーザまたはグループを指定できます。デフォルトでは、これは*SuperAdmins*のグループになります。ユーザを追加する方法は、*定義とユーザ* > *ユーザとグループ* > *ユーザ*ページで説明しています。

許可ネットワーク: *許可ネットワーク*ボックスで、WebAdminインタフェースに接続できるネットワークを定義できます。をスムーズにインストールするために、デフォルトはUTM*すべて*になっています。これは、WebAdminインタフェースはどこからでもアクセスできることを意味します。この設定は、できるだけ早く内部ネットワークに変更してください。ただし、最もセキュアなソリューションは、アクセスを、HTTPS経由の1台の管理者用PCのみに制限することです。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

アクセストラフィックをログ: すべてのWebAdminアクセスアクティビティをファイアウォールログにログする場合は、*アクセストラックをログ*チェックボックスにチェックを入れます。

4.2.2 アクセス制御

WebAdmin設定 > *アクセス制御タブで、特定のユーザに対してWebAdmin*ロールを作成することができます。これにより、WebAdminユーザに付与できる権限を細かく定義することができます。

以下の2つのユーザロールがあらかじめ定義されています。

AUDITOR 監査担当者 : このロールのユーザは、ログデータやレポートデータを参照できます。

READONLY 読取専用 : このロールのユーザは、WebAdmin内のすべてを参照できますが、編集、作成、削除は一切できません。

これらのいずれかの役割をユーザまたはグループに割り当てるには、*編集*ボタンをクリックし、各ユーザまたはグループを*メンバ*ボックスに追加します。

セキュリティポリシに応じて、追加の役割を作成することができます。次の手順で実行します:

1. ***アクセスコントロール*タブで、*新規役割*をクリックします。**
   *役割の追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前: この定義を説明する名前を入力してください。

メンバ：このロールを割り当てるユーザまたはグループを追加または選択します。ユーザを追加する方法は、*定義とユーザ* > *ユーザとグループ* > *ユーザ*ページで説明しています。

読取専用アクセスのみ許可（オプション）：このチェックボックスにチェックを入れると、WebAdminのすべてのエリアへの読取専用アクセスが、指定メンバに付与されます。

権限：このボックスでは、WebAdminの異なる職種に対し、異なる権限レベルが含まれています：Auditor：監査担当者とManager：管理者。Managerは各機能に対する完全な管理権限を持ちますが、Auditorは参照権限のみです。権限の前にあるチェックボックスにチェックを入れて、1つ以上の権限を選択することができます。

ユーザJon Doeに、メールプロテクションのManager権限を付与し、追加で*読取専用アクセスを付与*チェックボックスにチェックを入れるとします。このユーザは、メールプロテクションのセクションでは設定を変更できますが、WebAdminのその他のエリアでは参照のみ可能で、変更は一切できません。

コメント（オプション）：説明などの情報を追加します。

3. ***保存*をクリックします。**
   設定が保存されます。

役割を編集または削除するには、対応するボタンをクリックします。*AUDITOR*と*READONLY*の各ロールは削除できません。

4.2.3 HTTPS証明書

マネジメント > *WebAdmin設定* > *HTTPS証明書*タブで、WebAdmin CA証明書をブラウザにインポートしたり、WebAdmin証明書を再生成したり、WebAdminとユーザポータルでの署名証明書の使用を選択したりできます。

WebAdminアクセスの初回セットアップ時に、ローカルCAUTM証明書をで作成しました。このCA証明書の公開鍵をお使いのブラウザにインストールすると、WebAdminインタフェースへのアクセス時にセキュリティ警告が表示されなくなります。

CA証明書をインポートするには、以下の手順に従います。

1. ***HTTPS証明書*タブで*CA証明書をインポート*をクリックします。**
   CA証明書の公開鍵がエクスポートされます。

   CA証明書の公開鍵は、ディスクに保存するか、お使いのブラウザにインストールできます。

2. **証明書をインストールします** *オプション* **。**
   ブラウザにダイアログボックスが表示され、証明書のインストールをすぐに選択できます。

注 – システム時刻とタイムゾーンの違いによって証明書を作成してもすぐに有効にならない場合があります。この場合、ほとんどのブラウザでは、証明書が期限切れであると表示されますが、この表示は間違っています。ただし、証明書は24時間以内には自動的に有効になり、その後27年間有効期間が持続します。

WebAdmin証明書の再生成

WebAdmin証明書は、お客様が初回ログイン時に指定したホスト名を参照します。その間にホスト名が変更された場合は、ブラウザがセキュリティ警告を表示します。この問題を避けるために、新しいホスト名を考慮に入れて証明書を作成できます。このようなホスト名を入力して*適用*をクリックします。証明書の変更後、WebAdminで引き続き作業を行うには、多くの場合、お使いのWebブラウザでページをリロード(再読み込み)し、新しい証明書を承認して、WebAdminに再度ログインする必要があります。

WebAdmin/ユーザポータル証明書を選択してください

CA証明書をインポートする代わりに、独自に署名した証明書をWebAdmin/ユーザポータルで使用したい場合、ここでその証明書を選択します。ただし、ドロップダウンリストで証明書を選択できるようにするためには、最初に*リモートアクセス > 証明書管理 > 証明書*タブにおいて、証明書、CA、秘密鍵が含まれる証明書をPKCS#12形式でアップロードする必要があります。アップロードされた証明書を使用するには、*証明書*ドロップダウンリストから選択し、*適用*をクリックします。

4.2.4 ユーザ設定

*マネジメント > WebAdmin設定 > ユーザ設定*タブで、現在ログインしているユーザのためにグローバルショートカットやページあたりのアイテムといったユーザプリファレンス(基本設定)を構成できます。

WebAdminショートカット設定

*ここでは、多くの設定に使用されるドラッグ&ドロップのオブジェクトリストを開いたり閉じたりするためのキーボードショートカットを設定できます(詳細は、**WebAdmin > オブジェクトリストを参照)**。また、検索ボックスのカーソルフォーカスを設定できます**WebAdmin > WebAdmin メニュー*を参照)。ドロップダウンリストを使用して、Alt、Ctrl、Shiftなどの各種修飾キーとテキストボックスを選択し、異なる文字を入力してください。また、ドロップダウンリストで*オフ*を選択して、キーボードショートカットをオフにできます。

デフォルトの設定に戻るには、*出荷時設定にリセット*ボタンをクリックします。設定を保存するには*適用*をクリックします。

テーブルページャオプション

ここでWebAdminのテーブルのページネーション（ページ割り）、つまり、ページあたりのアイテムの表示数をグローバルに定義できます。ドロップダウンリストをクリックして値を選択します。設定を保存するには*適用*をクリックします。

WebAdminブラウザタイトルのカスタマイズ

ここでは、WebAdminブラウザのウィンドウまたはタブに表示するラベルを変更できます。プレーンテキストを入力するか、次の変数を使用できます。

- %h：ホスト名
- %u：ユーザ名
- %i：リモートIP アドレス

デフォルト設定は、`WebAdmin - User %u - Device %h`で、*WebAdmin - User admin - Device asg.example.com*のように表示されます。設定を保存するには*適用*をクリックします。

4.2.5 詳細

WebAdminアイドルタイムアウト

待ち時間：このフィールドでは、どれぐらいWebAdminセッションのアイドル期間が続いたら管理者に再度ログインを要求するかを秒単位で指定できます。デフォルトでは、アイドルタイムアウトは1,800秒に設定されています。指定できる範囲は60～86,400秒です。

ダッシュボード画面でもログアウト：WebAdminの*ダッシュボード*ページを開くと、自動ログアウト機能はデフォルトで有効になっています。ただし、このオプションを選択して、自動ログアウト機能をダッシュボードでのみ、無効化することができます。

WebAdmin TCPポート

デフォルトでは、ポート`4444`をWebAdminのTCPポートとして使用します。*TCPポート*ボックスには、`443`あるいは`1024`～`65535`の任意の値を入力できます。ただし、一部のポートは他のサービス用に予約されています。特に、ポート`10443`は使用できません。また、ユーザポータルあるいはSSLリモートアクセスに使用しているものと同じポートは使用できません。WebAdminにアクセスするときは、ブラウザのアドレスバーでポート番号をIPアドレスに（コロンで区切って）追加する必要があります。例えば、`https://192.168.0.1:4444`のように指定します。

利用規約

会社ポリシで、WebAdminへのアクセスを求めるユーザに利用規約への同意を求めることができます。ユーザがWebAdminにログインするたびに利用規約に同意することを要求するには、*ログイン後に「利用規約」を表示*チェックボックスにチェックを入れます。これにより、ユーザーがログインすると利用条件が表示されるようになります。利用条件に同意しないと、再びログアウトされます。

必要に応じて利用規約の文面を変更することができます。設定を保存するには*適用*をクリックします。

Sophos Adaptive Learning

現在の設定に関する一般的な匿名情報や検出されたウイルス、または匿名指紋をSophosに転送することで、Sophos UTMの改善にご協力ください。この種の情報からユーザを特定することはありません。また特定することもできません。ユーザ固有の情報、つまりユーザ名、オブジェクト名、コメント、その他の個人情報を収集することはありません。ただし、Webフィルタのウイルス対策スキャンが有効であると、ウイルスが検出されたURLは転送されます。

情報は、SSLにより暗号化してSophosラボに送信されます。送信されたデータは集計形式で保存されます。Sophosのソフトウェアアーキテクトは、このデータを基に設計関連の決定を行い、将来のバージョンのSophos UTMの向上に役立てます。

匿名テレメトリデータを送信:有効であると、UTMは、以下の情報を収集します:

- 設定および使用のデータ:システムは、以下のデータをSophosのサーバに毎週一度送信します。
    - 次のようなハードウェアおよびライセンス情報(所有者を除く):

      ```
      processor Intel(R) Core(TM)2 Duo CPU E8200 @ 2.66GHz
      memory 512MiB System Memory
      eth0 network 82545EM Gigabit Ethernet Controller
      id: UTM
      バージョン: 9.000000
      バージョン: 4.000000
      タイプ: 仮想
      ライセンス: 標準
      モード: スタンドアロン
      active_ips:2
      system_id:58174596-276f-39b8-854b-ffa1886e3c6c
      ```

システムIDは、再インストールの後などに、システム情報が誤って2回収集されることがないように確認できる範囲のみでUTMを識別します。

- 次のような機能の使用状況（有効か無効かの特定のみ）:

  ```
  main->backup->status:1
  main->ha->status:オフ
  ```

- 次のような設定オブジェクトの数:

  ```
  objects->interface->ethernet: 2
  objects->http->profile: 5
  ```

- 有効化されたWebフィルタリングカテゴリおよび除外
- CPU、メモリおよびスワップ使用状況（%）に関する過去7日の値

- ウイルスデータ:システムは、以下のデータをファイルに書き込みます。このファイルは、15分毎にSophosのサーバにアップロードされます。
  - たとえば、名前、MIMEタイプ、リクエストのURL、ファイルサイズなどのWebプロテクションで検出されたウイルスに関する情報。
- 侵入防御データ:IPSログで、新しいアラートを毎分毎にチェックします。新しいアラートがあると、以下のデータがただちにSophosに送信されます:
  - snortルール識別子やタイムスタンプなどのアラートに関する情報。
  - ハードウェアおよびライセンス情報（所有者を除く）例:CPUトータル、CPU使用状況、メモリトータル、メモリ使用状況、SWAPトータル、SWAP使用状況、システムID、Engineのバージョン、パターンのバージョンなど。

    データは、24時間ごとに送信されます。
- 高度な脅威防御データ:システムは、高度な脅威防御データを30分毎に生成し、アップロードします。
  - 収集情報:システムID、タイムスタンプ、Sophos脅威名、ソースIP、宛先ホスト、検出コンテンツ、検出詳細、脅威数、ルール識別子。

匿名アプリケーション正確性遠隔測定データの送信:**Sophos UTMAppAccuracy**プログラムに参加すると、ネットワークの可視性とアプリケーション制御の認識と分類の向上に貢献いただけます。有効であれば、このシステムは、匿名のアプリケーション指紋という形でデータを収集し、Sophosのリサーチチームへ送信します。ここでは、指紋を使用して、未分類のアプリケーションを識別し、ネットワーク可視化およびアプリケーションコントロールライブラリを改良および拡張します。

4.3 ライセンス

Sophos UTMの特定の機能を使用できるか否かは、ライセンスとサブスクリプションによって定義されています。UTMつまり、とともに購入したライセンスとサブスクリプションに応じて、一部の機能は使用でき、他の機能は使用できなくなります。

4.3.1 ライセンスの取得方法

Sophos UTMには、すべての機能が有効になる30日間のトライアルライセンスが付属しています。このライセンスの期限満了後にSophos UTMを操作したい場合には、有効なライセンスをインストールする必要があります。すべてのライセンス（無料のホームユーザーライセンスを含む）はMyUTM ユーザガイドで作成されます。

UTMライセンスの購入後に、アクティベーションキーがメールで送信されます。これらのキーを使用して、ライセンスを作成するか、既存のライセンスをアップグレードしてください。ライセンスを有効にするには、MyUTM ユーザガイドにログインし、ライセンス管理のページにアクセスしてください。ページ上部にあるフォームの該当フィールドに、メールからアクティベーションキーをカット＆ペーストします。詳しくは、MyUTMユーザガイドを参照してください。

MyUTM Licensing Portal

The MyUTM portal allows you to manage your product licenses and request technical support. Enter your credentials to log in, or create an account below.

Log in

Enter your e-mail address:

Enter your password:

Access MyUTM

If you have forgotten your password, please click here and a new password will be sent to your inbox.

Create a MyUTM Account

Join today and get instant access. You can manage your product licenses here. Plus, you'll get a free, fully-functional home use license for Sophos UTM.

MyUTM Support

If you have any problems with your account credentials or need to be upgraded to partner status, please email us at nsglicensing@sophos.com.

© 2013 Sophos Ltd. All rights reserved. Legal Privacy End User License Agreement Cookie Information

図 **8** MyUTMポータル

別のフォームが表示されます。ここで、お客様がライセンスを購入した代理店についての情報と、お客様自身の詳細情報を入力してください。このフォームには、わかる限りの情報があらかじめ入力されています。また、該当する場合、SophosはUTMハードウェアのシリアル番号をこのフォームから収集します。フォームの送信後、ライセンスが作成され、ライセンス詳細ページが表示されます。ここで、ライセンスファイルをダウンロードすることができます。

ライセンスを実際に使用する場合、ライセンスファイルをハードドライブにダウンロードして、インストールされているWebAdminにログインする必要があります。WebAdminで、*マネジメント* > *ライセンス* > *インストレーション*タブにアクセスし、アップロード機能を使用してハードドライブ上のライセンステキストファイルを検索します。ライセンスファイルをアップロードすると、WebAdminがこれを処理して、すべてのサブスクリプションと、ライセンスに規定されたその他の設定を有効にします。

注 – メールで受信したアクティベーションキーをWebAdminにインポートすることはできません。このキーは、ライセンスの有効化だけに使用されます。UTMにインポートできるのはライセンスファイルのみです。

4.3.2 ライセンスモデル

Sophosのモジュール式ライセンスモデルは非常に柔軟です。まず、基本ライセンスでは、基本機能を無料で提供しています(下の表を参照)。次に、6種類の追加サブスクリプションがあります。

- ネットワークプロテクション
- Webプロテクション
- Eメールプロテクション
- エンドポイントプロテクション
- ワイヤレスプロテクション
- Webサーバープロテクション

これらは、ニーズに合わせて個別に購入することも組み合わせて購入することもできます。FullGuardライセンスにはすべてのサブスクリプションが含まれています。それぞれのサブスクリプションを使用して、製品の特定の機能を利用できます。下の表は、どのサブスクリプションでどの機能を使用できるかを示しています。

機能	基本ライセンス	ネットワーク	Web	Eメール	エンドポイント	ワイヤレス	Webサーバー
管理　バックアップ、通知、SNMP、SYMなど	✓						
ローカル認証　ユーザー、グループ	✓						
基本ネットワーキング　スタティックルート、DHCP、DNS、Auto QoS、NTPなど	✓						
ファイアウォール/NAT　DNAT、SNATなど	✓						
PPTP & L2TP リモートアクセス	✓						
ローカルログ、標準エグゼクティブレポート	✓						
侵入防御　パターン、DoS、フラッド、ポートスキャンなど		✓					
IPsec & SSL サイト間 VPN、IPsec & SSL リモートアクセス		✓					

機能	基本ライセンス	ネットワーク	Web	Eメール	エンドポイント	ワイヤレス	Webサーバー
アドバンストネットワーキング リンクアグリゲーション、リンクバランシング、ポリシールーティング、OSPF、マルチキャスト、カスタムQoS、サーバロードバランシング、ジェネリックプロキシなど		✓	(✓)	(✓)			
ユーザポータル		✓	✓	✓			
冗長化		✓	✓	✓			
リモート認証 AD、eDir、RADIUSなど		✓	✓	✓			
リモートログ、詳細エグゼクティブレポート アーカイブ、設定		✓	✓	✓			
基本Webフィルタリング&FTPプロキシ			✓				
Web&FTPマルウェアフィルタリング			✓				
アプリケーションコントロール			✓				

機能	基本ライセンス	ネットワーク	Web	Eメール	エンドポイント	ワイヤレス	Webサーバー
基本SMTPプロキシ、隔離レポート、メールマネージャ				✓			
SMTP & POP3マルウェアフィルタリング				✓			
エンドポイントプロテクション、ウイルス対策					✓		
エンドポイントプロテクション、デバイスコントロール					✓		
ワイヤレスプロテクション						✓	
Webサーバープロテクション							✓

また、UTMアプライアンス モデル100で選択可能なベーシックガードサブスクリプションもあります。これは、上記の基本機能を提供します（詳細は製品情報ページを参照してください）。

UTM機器はSophos UTM Manager（SUM）経由で一括管理およびライセンス許可できます。この場合、SUMがMSP（Managed Service Provider）ライセンスをUTMに提供し、*インストール*タブは無効化されます。サブスクリプションはSUMサービスプロバイダーによってのみ有効化できます。

サブスクリプションとその機能セットについて詳しくは、認定UTMパートナーまたはSophos UTM Webサイトまでお問い合わせください。

サブスクリプションがないと、WebAdminのタブが無効になります。タブの上には、ライセンス警告メッセージが表示されます。
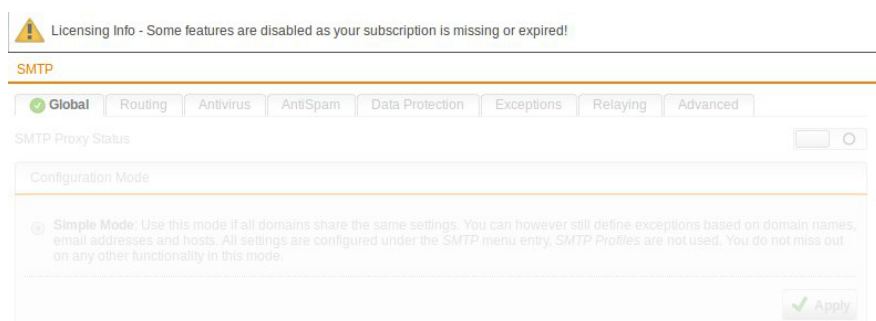
図 **9** ライセンス：サブスクリプション警告メッセージ

Up2Date

つまり、新しいファームウェアの更新に関する情報が自動的に通知されます。各サブスクリプションは、自動更新を完全にサポートします。つまり、また、ファームウェアとパターン更新を自動的にダウンロード(およびインストール)できます。

サブスクリプションなしの基本ライセンスでは、自動更新に制限があります。オンラインヘルプの更新などのパターン更新に限り、自動的にダウンロードされ、インストールされますが、使用可能なファームウェア更新については通知されず、ファームウェア更新は手動でダウンロードする必要があります。新しいファームウェアの通知は、Sophos UTMUp2Dateブログに表示されます。

サポートとメンテナンス

基本ライセンスには*Web* *サポート*が含まれます。Sophos UTM サポートフォーラムおよびSophos Knowledgebaseを使用できます。

いずれかのサブスクリプションを購入すると、すぐに*標準サポート*に自動的にアップグレードされます。これにより、さらにMyUTM ユーザガイドでサポートを受けたり、認定済みのUTMパートナーに問い合わせをすることができます。

UTMエンジニアが担当者として24時間年中無休のサポートを提供する*プレミアムサポート*サブスクリプションを購入することもできます。

4.3.3 概要

ライセンス > *オーバビュー*タブには、*ライセンス*に関する詳細情報が表示され、次のように複数のエリアに分割されています。

- 基本 ライセンス: ID、登録日、タイプなどの基本的なライセンスパラメータが表示されます。
- ネットワークプロテクション、**E** メールプロテクション、**Web**プロテクション、**Web** サーバプロテクション、ワイヤレスプロテクション、エンドポイントウイルス対策、ベーシックガード: サブスクリプションに関する情報(購入したものか否か、有効化されているか、有効期限、および提供する機能の簡単な説明など)が表示されます。

  注 **–** MSPライセンスを使用する場合、ライセンスはSophosUTM Manager (SUM)によって管理されるので、有効期限は表示されません。従来のキーおよびサブスクリプションは、SUM MSPシステムによって置き換えられます。SUMの管理の詳細は、*集中管理* > *Sophos UTM Manager*を参照してください。

- サポートサービス: サポートレベルと有効期限が表示されます。

4.3.4 インストール

マネジメント > *ライセンス* > *インストール*タブでは、新しいライセンスのアップロードおよびインストールを実行できます。

注 **–** MSP ライセンスを使用する場合、ライセンスはSophos UTM Manager (SUM)によって管理されるので、このタブは無効になります。新しいライセンスは、SUMサービスプロバイダによってインストールされます。SUMの管理の詳細は、*集中管理* > *Sophos UTM Manager*を参照してください。

ライセンスをインストールするには、次の手順に従ってください。

1. ***ファイルのアップロード*ダイアログウィンドウを開きます。**
   *ライセンスファイル*ボックスの横にあるフォルダアイコンをクリックします。

   *ファイルのアップロード*ダイアログウィンドウが開きます。

2. **ライセンスファイルを選択します。**
   ライセンスファイルが保存されているディレクトリを参照します。

   アップロードするライセンスファイルを選択します。

3. ***アップロード開始*をクリックします。**
   ライセンスファイルがアップロードされます。

4. ***適用*をクリックします。**

ライセンスがインストールされます。新しいライセンスは、すでにインストールされている他のライセンスを自動的に置き換えます。

ライセンスのインストールには約60秒かかります。

4.3.5 アクティブなIPアドレス

Sophos UTM Managerの無料ライセンスでは、IPアドレスは無制限です。

ユーザ（IPアドレス）が無制限に許可されるライセンスをお持ちでない場合は、お客様のライセンスでカバーされるIPアドレスに関する情報がこのタブに表示されます。お客様のライセンスの範囲外となるIPアドレスは、別のリストに記載されています。制限を超えると、定期的にEメール通知が送信されます。

注 – 7日間にわたって使用されなかったIPアドレスは、ライセンスカウンタから自動的に削除されます。

4.4 Up2Date

*マネジメント > Up2Date*メニューを使用して、Sophos UTMの更新サービスを設定できます。定期的に更新パッケージをインストールすることで、UTMをバグフィックス、製品改善機能、ウイルスパターンなどが最新に保たれます。各更新パッケージは、Sophosによってデジタル署名されています。署名がないものや偽造された更新は拒否されます。デフォルトでは新しい更新パッケージは自動的にUTMにダウンロードされます。このオプションは、*マネジメント > Up2Date > 設定*メニューで設定できます。

2種類の更新を利用できます。

- ファームウェアの更新：ファームウェアの更新には、Sophos UTMソフトウェアのバグフィックスおよび拡張機能が含まれています。
- パターンの更新：パターンの更新によって、ウイルス対策、スパム対策、IPSのルール、およびオンラインヘルプが最新状態に保たれます。

Up2Dateパッケージをダウンロードするために、UTMは更新サーバに対するTCP接続をポート443で開きます。このため、この接続は管理者の調整なしで使用できます。ただし、途中に別のファイアウォールがある場合は、ポート443 TCPを介した更新サーバへの通信を明示的に許可する必要があります。

4.4.1 概要

*マネジメント > Up2Date > 概要*タブには、お使いのシステムが最新のものであるかどうかを示す概要が表示されます。ここで、新しいファームウェアやパターンの更新パッケージをインストールできます。

Up2Date進行状況

ここで、新しいファームウェアやパターンの更新パッケージをインストールできます。*Up2Dateの進行状況を新しいウィンドウで確認する*ボタンをクリックして、更新の進行状況をモニタしてください。ブラウザでポップアップウインドウの表示を禁止していない限り、更新の進行状況を示す新しいウインドウが表示されます。表示されない場合は、ポップアップウインドウを明示的に許可する必要があります。

注 – インストールプロセスが開始する前に、標準バックアップメール受信者にバックアップが送信されます。
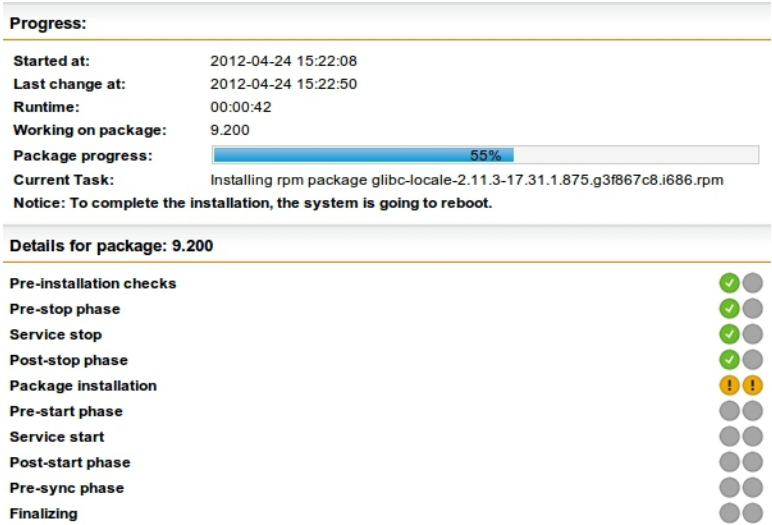
図 **10** Up2Date:進捗ウィンドウ

ファームウェア

*ファームウェア*セクションには、現在インストールされているファームウェアのバージョンが表示されます。更新パッケージが利用できる場合は、*すぐに最新バージョンに更新*ボタンが表示されます。また、*利用可能なファームウェアの概要*セクションにメッセージが表示されます。ここで最新の更新パッケージを直接ダウンロードしてインストールできます。*すぐに最新バージョンに更新*をクリックすると、新しいウインドウに更新の進行状況が表示されます。これには、Webadmin *リロード*ボタンをクリックします。

利用可能なファームウェアUp2Date

*設定*タブで*手動*を選択すると、このセクションに*すぐにUp2Dateパッケージを確認*ボタンが表示されます。このボタンを使用して、ファームウェアのUp2Dateパッケージを手動でダウンロードできます。Up2Dateが複数利用できる場合は、どれをインストールするかを選択できます。最も新しいバージョンを直接インストールしたい場合は、*ファームウェア*セクションの*すぐに最新バージョンに更新*ボタンを使用します。

各Up2Dateには*スケジュール*ボタンがあり、更新パッケージを自動的にインストールする日時を指定できます。スケジュールしたインストールを取り消す場合は、*キャンセル*をクリックします。

「暗黙的」インストールに関する注記：スケジュールしたUp2Dateパッケージが、古いUp2Dateパッケージを最初にインストールすることを必要とする場合があります。その場合、この古いUp2Dateパッケージは、実際のUp2Dateパッケージの前にインストールするよう自動的にスケジュールされます。このパッケージに特定のタイミングを指定することもできますが、そのインストールを止めることはできません。

パターン

*パターン*セクションには、インストールしたパターンの現在のバージョンが表示されます。*設定*タブで*手動*を選択すると、*すぐにパターンを更新*ボタンが表示されます。このボタンを使用して、使用可能な新しいパターンをダウンロードしてインストールします。

注 – UTMユニットを正常に動作させるために、現在のパターンバージョンと利用可能な最新のパターンバージョンが一致している必要はありません。お使いのユニットに新しいパターンを適用できない場合は、現在のパターンバージョンと利用できる最新パターンバージョンが異なってきます。どのパターンをダウンロードするかは、お客様の設定とハードウェアの構成によります。たとえば、Sophos UTMのIPS機能を使用しない場合は、新しく利用可能になったIPSパターンはインストールされません。このようにして、現在インストールされているパターンバージョンと利用できる最新のパターンバージョンの開きが大きくなっていきます。

4.4.2 設定

デフォルトでは、新しい更新パッケージは自動的にUTMにダウンロードされます。

ファームウェアのダウンロードを行う間隔

このオプションは、デフォルトで15分に設定されています。つまり、Sophos UTMは、15分毎に利用できるファームウェアの更新を確認します。Sophos UTMは、利用できるファームウェア更新パッケージを自動的にダウンロードします(インストールは行いません)。これが行われる実際の時間は、選択された間隔の制限内でランダムに決定されます。最長で*マンスリー*の間隔を指定できます。または、ドロップダウンリストから*手動*を選択することで、ファームウェアの自動ダウンロードを無効にできます。*手動*を選択した場合は、*すぐにUp2Dateパッケージを確認*ボタンが*概要*タブに表示されます。

パターンのダウンロード/インストールを行う間隔

このオプションは、デフォルトで15分に設定されています。つまり、Sophos UTMは、15分毎に利用できるパターン更新を確認します。Sophos UTMは、利用できるパターン更新パッケージを自動的にダウンロードしてインストールします。これが行われる実際の時間は、選択された間隔の制限内でランダムに決定されます。最長で*マンスリー*の間隔を指定できます。または、ドロップダウンリストから*手動*を選択することで、パターンの自動ダウンロードとインストールを無効にできます。*手動*を選択した場合は、*すぐにパターンを更新*ボタンが*概要*タブに表示されます。

4.4.3 詳細

*マネジメント > Up2Date > 詳細*タブで、詳細なUp2Dateオプションを設定できます。たとえば、UTM用に親プロキシまたはUp2Dateキャッシュを選択することなどができます。

> **注 –** 更新パSophos UTM FTP サーバッケージはからダウンロードできます。

手動Up2Dateパッケージアップロード: UTMが新規更新パッケージを直接ダウンロードするためにインターネットまたはUp2Dateキャッシュに直接アクセスできない場合は、更新パッケージを手動でアップロードできます。手動でアップロードするには、以下の手順に従います。

1. ***ファイルのアップロード*ダイアログウィンドウを開きます。**

   *Up2Date ファイル*ボックスの横にあるフォルダアイコンをクリックします。

   *ファイルのアップロード*ダイアログウィンドウが開きます。

2. **更新パッケージを選択します。**
   *ファイルのアップロード*ダイアログボックスの*参照*をクリックして、アップロードする更新パッケージを選択します。

3. ***アップロード開始*をクリックします。**
   更新パッケージがUTMにアップロードされます。

4. ***適用*をクリックします。**
   設定が保存されます。

親プロキシ

親プロキシは、多くの場合、政府承認のプロキシサーバを通してインターネットアクセスをルーティングする必要のある国で必要とされます。親プロキシの使用がセキュリティポリシで求められている場合、ここでホスト定義とポートを選択して親プロキシを設定できます。

親プロキシを使用:

1. 親プロキシの使用を有効にするには、チェックボックスにチェックを入れます。

2. ホストを選択または追加します。

3. **プロキシのポートを入力します。**
   定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

4. ***適用*をクリックします。**
   設定が保存されます。

プロキシ認証を使用:親プロキシで認証が必要な場合、ここでユーザ名とパスワードを入力します。

> 注 - *集中管理* > *Sophos UTM Manager*タブで、*SUMサーバをUp2Dateキャッシュとして使用*オプションが有効化されている場合、親プロキシは無効となります。

親プロキシが設定されている場合は、Sophos UTMはファームウェアとパターンのUp2Dateの両方を親プロキシからフェッチします。

4.5 バックアップ/リストア

バックアップ/リストア機能を使用すると、UTMの設定をローカルディスク上のファイルに保存することができます。このバックアップファイルを使用すると、新しいシステムや設定が誤っているシステ

ムに、適切であるとわかっている設定をインストールすることができます。

システムに変更を加えるたびに忘れずにバックアップをとってください。これにより、常に最新の設定を使用できるようになります。さらに、バックアップは安全な場所に保存してください。この理由は、証明書や暗号化鍵といったセキュリティ関連のデータも含まれているためです。バックアップの生成後、読み取り可能であることを必ずチェックしてください。外部プログラムを使用してMD5チェックサムを生成すると良いでしょう。これにより、バックアップの完全性を後でチェックすることができます。

4.5.1 バックアップ/リストア

*マネジメント > バックアップ/リストア > バックアップ/リストア*タブでは、バックアップの作成やインポートに加え、既存のバックアップのリストア、ダウンロード、送信、削除ができます。

利用可能なバックアップ

このセクションは、自動バックアップ機能か手動により以前に1つ以上のバックアップが作成されている場合にのみ表示されます(*バックアップの作成*のセクションを参照してください)。

すべてのバックアップが、作成日時、UTMバージョン番号、作成ユーザー、コメントと共にリストされます。

バックアップに対して、ダウンロード、リストア、削除、送信を実行できます。

- **ダウンロード:** 開いたダイアログウィンドウで、暗号化されたファイル(パスワードを指定)または暗号化されていないファイルのダウンロードを選択できます。*バックアップのダウンロード*をクリックします。ダウンロードするバックアップを保存するファイルシステム内の場所を選択するよう求められます。
  - **ダウンロード前に暗号化:** バックアップのダウンロードまたは送信の前に、バックアップを暗号化することもできます。CBCモードでの暗号化は、Blowfish暗号によって行われます。パスワードを入力します(確認のために2回入力します)。バックアップのインポート時に、このパスワードが求められます。暗号化されたバックアップのファイル拡張子は`ebf`、暗号化されていないバックアップのファイル拡張子は`abf`です。

    注 - バックアップには、管理者パスワード、HAパスフレーズ(設定している場合)、すべてのRSA鍵およびX.509証明書が含まれます。これは機密情報なので、暗号化を有効にするのが賢明です。

- **リストア:** 現在のシステム設定をバックアップに保存されている設定に変更します。リストア

後に再度ログインする必要があります。選択したバックアップにすべてのデータが含まれている場合、すぐにログインできます。選択したバックアップにすべてのデータが含まれていない場合（*バックアップの作成*のセクションを参照）、ログイン過程で必要なデータを入力する必要があります。選択したバックアップでホストデータのみが削除されている場合は、必要に応じて管理者のメールアドレスを追加することができます。この情報は受信者が指定されていない場合に使用されるか、複数受信者を指定できる場合に追加アドレスとして使用されます。

注 – バックアップリストアは後方互換性のみがあります。現在のバージョンより古いものからのバックアップのみが、機能するものと見なされます。バージョンの対立がある場合、*使用可能なバックアップ*リスト内のバージョン番号がオレンジになります。

- USBフラッシュドライブからのバックアップのリストア：USBスティックなどのFATフォーマットされたUSBフラッシュドライブから、暗号化されていないバックアップファイル（ファイル拡張子abf）をリストアすることもできます。USBフラッシュドライブからバックアップをリストアするには、バックアップファイルをUSBフラッシュドライブにコピーして、ブート（起動）前にデバイスをSophos UTMにプラグインします。デバイスに複数のバックアップファイルが保存されている場合、辞書的に最初のファイルが使用されます（数字は文字より優先します）。たとえば、バックアップファイルであるgateway_backup_2012-04-17.abfと2011-03-20_gateway_backup.abfの両ファイルがUSBフラッシュドライブに保存されているとします。ブート時に使用されるのは2つ目のファイルです。このファイルはもう一方より日時が古いのですが、ファイル名の先頭が数字であるためです。

  さらに、バックアップのリカバリが成功するとロックファイルが作成され、USBフラッシュドライブが接続されている間に同じバックアップが何度も繰り返しインストールされることを防ぎます。前のバックアップを再びインストールしたい場合には、USBフラッシュドライブをプラグインしていない状態でリブート（再起動）する必要があります。これにより、すべてのロックファイルが削除されます。再びUSBフラッシュドライブを接続してからブートすると、同じバックアップをインストールすることができます。

- 削除：リストからバックアップを削除します。リストの最下部にある削除アイコンを使用して、選択したバックアップをすべて削除することができます。バックアップを選択するには、バックアップの左にあるチェックボックスをクリックするか、最下部にあるチェックボックスを使用してすべてのバックアップを選択します。

- 送信：ダイアログウィンドウで、メール受信者を指定することができます。デフォルトでは、*自動バックアップ*タブで指定したアドレスが選択されています。次に、ファイルを暗号化して（パスワードとともに）送信するか、暗号化せずに送信するかを決めることができます。*直ち*

*に送信*をクリックしてバックアップを送信します。

- **送信前に暗号化:**前述の*ダウンロード前に暗号化*を参照してください。

バックアップの作成

バックアップは、(予期しない)変更または故障の後でシステムをリストアするために便利なだけではありません。類似の設定にするシステムをセットアップする際のテンプレートとして使用し、これらのシステムをあらかじめある程度設定しておくことで、時間を大幅に節約できます。そのためには、バックアップを作成する前に、ホスト名、証明書など特定の情報を削除しておくことができます。

現在のシステム状態のバックアップを作成するには、次の手順に従います。

1. *バックアップの作成*セクションに、**コメントを入力します** *オプション* 。
   コメントは、バックアップリストでバックアップとともに表示されます。

2. **次の設定を行います** *オプション* 。
   サイト固有情報を削除する:ホスト固有のデータなしでバックアップを作成するには、このオプションを選択します。この対象となるのは、ホスト名、システムID、SNMPデータ、HAデータ、ライセンス、シェルユーザパスワード、匿名パスワード、ならびにメールプロテクション、Webプロテクション、クライアント認証、IPsec、SSL VPN、RED、WebAdmin、Webアプリケーションファイアウォール、およびプロキシ用のすべての証明書、公開鍵と秘密鍵、および指紋とシークレットなどです。

   このようなバックアップは、類似のシステムを複数セットアップするために便利です。ただし、いくつか考慮すべき点があります。1)リストア後は、基本システムセットアップになります。2)最初のインタフェースのみが設定されています。プライマリIPアドレスは、インストール中に構成される設定の1つです。他のすべてのインタフェースは無効になり、IPアドレスが`0.0.0.0`に設定されます。

   > **警告** - ほとんどのホスト固有データが削除されても、このようなバックアップテンプレートにはユーザパスワードなどの機密情報がまだ含まれています。そのため、必ず暗号化することをお勧めします。

   管理メールメッセージの削除:UTMの様々な部分(メールプロテクションのポストマスタアドレス、通知など)で使用される管理者のメールアドレスを追加で削除するには、このオプションを選択します。このオプションは、Sophos UTM顧客のサイトでデバイスをセットアップするITパートナーにとって特に便利です。

3. *バックアップを直ちに作成*を**クリックします。**
   使用可能なバックアップのリストに、バックアップが表示されます。

これらのオプションのいずれかまたは両方を選択してバックアップを作成した場合には、バックアップエントリにそれぞれの追加コメントが含まれるようになります。

注 – HA設定は、ハードウェア設定の一部であり、バックアップ内に保存できません。これは、HA設定はバックアップリストアで上書きできないということを意味します。

バックアップのインポート

バックアップをインポートするには、次の手順に従ってください。

1. フォルダアイコンをクリックし、アップロードするバックアップファイルを選択します。
2. *アップロード開始*をクリックします。
3. **バックアップを復号化します。**
   暗号化されたバックアップファイルをアップロードする場合、バックアップのインポート前に、正しいパスフレーズを入力する必要があります。
4. ***バックアップのインポート*をクリックして、バックアップをインポートします。**
   バックアップはすぐにリストアされるのではなく、*使用可能なバックアップ*リストに追加されます。

4.5.2 自動バックアップ

*マネジメント > バックアップ/リストア > 自動バックアップ*タブでは、バックアップの自動生成に関する複数のオプションを設定することができます。バックアップを自動的に作成するためには、次の手順に従います。

1. ***自動バックアップ*タブで自動バックアップを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチが緑色になり、*オプション*および*バックアップをメール送信*エリアが編集可能になります。
2. **間隔を選択します。**
   自動バックアップは、さまざまな間隔で作成することができます。

   デイリー、ウィークリー、マンスリーから選択できます。
3. **保存する最大バックアップ数を指定します。**
   最大バックアップに達した時点で、最古の自動バックアップが削除されます。最大値に到達すると、一番古いバックアップが削除されます。

この対象となるのは、自動作成されたバックアップのみです。システム更新の前に手動で作成されたバックアップや 自動的に作成されたバックアップは削除されません。

4. ***適用*をクリックします。**
設定が保存されます。

トグルスイッチが緑色に変わります。

UTMのバックアップ作業を簡素化するために、バックアップ機能では、定義したメールアドレスのリストに対して、バックアップファイルをメールで送信することができます。

受信者：自動的に生成されたバックアップは、*受信者*ボックスに含まれるユーザに送信されます。複数のアドレスを追加できます。デフォルトでは、最初の管理者のメールアドレスが使用されます。

Eメールバックアップの暗号化：さらに、オプションでバックアップを暗号化できます（3DES暗号化）。

パスワード：*Eメールバックアップの暗号化*オプションを選択したら、パスワードを入力します（確認のために2回）。バックアップのインポート時に、このパスワードが求められます。

自動的に作成されたバックアップは、*作成者*を示す `System` フラグ付きで*バックアップ/リストア*タブの*使用可能なバックアップ*リストに表示されます。ここで、自分で作成したバックアップと同様に、リストア、ダウンロード、削除を実行できます。

4.6 ユーザポータル

Sophos UTMのユーザポータルは、許可されたユーザにパーソナルなメールおよびリモートアクセスサービスを提供するユニットの特別なブラウザベースアプリケーションです。ユーザポータルにアクセスするには、Sophos UTMのURL（`https://192.168.2.100`など）にブラウズします（HTTPSプロトコルを使用していることと、WebAdminインタフェースにアクセスするために通常入力するポート番号`4444`がないことに注意）。

ユーザポータルは、メール隔離を始めとする機能を備えています。メール隔離は、悪意あるソフトウェアに感染したメッセージ、不審な添付物を含むメッセージ、スパムと特定されたメッセージ、または明確に禁止した表現を含むメッセージを保持します。

ログインページで、ユーザはヘッダバーの右側にあるドロップダウンリストから言語を選択できます。
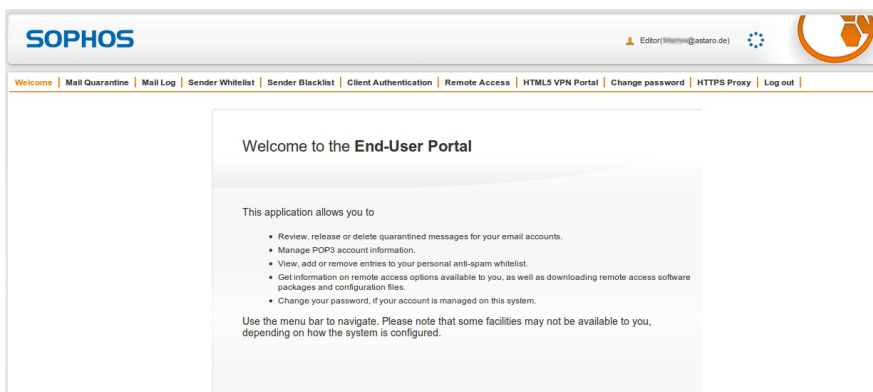
図 11 ユーザポータル:「ようこそ」のページ

ユーザポータルで、ユーザは以下のサービスにアクセスできます。

- **SMTP隔離**:ユーザは隔離場所に保持されているメッセージを表示したり、リリースできます。どのタイプのメッセージをユーザがリリースできるかは*Eメールプロテクション*>*隔離レポート*>*詳細*タブで決定できます。(このタブは、POP3が無効な場合は*メール隔離*となります。)
- **SMTP**ログ:ここでは、ユーザはメールトラフィックのSMTPログを表示できます。(このタブは、POP3が無効な場合は*メールログ*となります。)
- **POP3隔離**:ユーザは隔離場所に保持されているメッセージを表示したり、リリースできます。どのタイプのメッセージをユーザがリリースできるかは*Eメールプロテクション*>*隔離レポート*>*詳細*タブで決定できます。(このタブは、SMTPが無効な場合は*メール隔離*となります。)
- **POP3**アカウント:ユーザは使用するPOP3アカウントの資格情報を入力できます。POP3アカウントの資格情報が与えられたスパムメールのみがユーザポータルに表示されます。POP3アカウントの資格情報が保存されているユーザは、各Eメールアドレスについて個々の隔離レポートを受け取ります。許可されるPOP3サーバは*Eメールプロテクション*>*POP3*>*詳細*タブで指定する必要があります。
- 送信者ホワイトリスト:ここで送信者をホワイトリストに追加することで、それらの送信者から送信されたメッセージがスパムとして分類されないようにできます。ただし、ウイルスを伴うメールや、スキャン不能なメールは引き続き隔離されます。ホワイトリスト内の送信者は、有効なメールアドレス(例:`jdoe@example.com`)またはアスタリスクをワイルドカードとして使用して特定ドメインの全メールアドレス(例:`*@example.com`)を指定できます。ホワイトリストのエントリが完全に一致する場合、送信者ブラックリストのチェックは省略されます。

- 送信者ブラックリスト: ここで、ユーザがメール送信者をブラックリスト化することができます。例、`phishing@hotmail.com`, or whole domains, e.g. `*@hotmail.com`。ブラックリストは、システム内でSMTPとPOP3が使用されていれば、SMTPとPOP3の両方のメールに適用されます。ブラックリストに送信者を追加するには、「+」アイコンをクリックしてアドレスを入力し、チェックアイコンをクリックして保存します。

- ホットスポット: ここでユーザは、ホットスポットのアクセスデータを確認して管理できます。このタブは、特定のユーザに対して1つ以上のホットスポットが有効にされている場合にのみ使用できます。当日有効パスワードタイプのホットスポットには、現在のパスワードの表示と変更を行うことができます。バウチャータイプのホットスポットには、バウチャーの生成、印刷、エクスポート、削除を行うことができます。生成バウチャーのリストには、使用状況の情報が表示されます。詳細は、*ワイヤレスプロテクション* > *ホットスポット*を参照してください。

- クライアント認証 : ここでユーザは、SophosAuthentication Agent（SAA）のセットアップファイルをダウンロードできます。SAAはWebフィルタの認証モードとして使用できます。*クライアント認証*タブは、クライアント認証が有効化されている場合にのみ使用できます。詳細は、*定義とユーザ* > *クライアント認証*を参照してください。

- **OTP** トークン: ここUTMで、ユーザは、使用しているモバイルデバイスでのワンタイムパスワードサービスを設定するためのQRコードおよびそれぞれの詳細情報を検索できます。詳細は、*定義とユーザ* > *認証サービス* > *ワンタイムパスワード*を参照してください。

- リモートアクセス: ユーザはリモートアクセスクライアントソフトウェアおよびそれらに付属する設定ファイルをダウンロードできます。ただし、*リモートアクセス*タブは、その特定ユーザに対して最低1つのリモートアクセスモードが有効になっている場合のみ利用できます。

- **HTML5 VPN** ポータル : ここでユーザは、定義済みのサービスを使用して定義済みのホストへのVPN接続を確立することができます。このタブは、特定のユーザに対して1つ以上のVPN接続が有効にされている場合にのみ使用できます。詳細は、*リモートアクセス* > *HTML5 VPN ポータル*を参照してください。

- パスワードの変更 : ユーザはユーザポータルにアクセルするためのパスワードを変更できます。

- **HTTPS**プロキシ : ユーザはHTTP/SプロキシCA証明書をインポートし、セキュアWebサイトへの訪問時に表示されるエラーメッセージを回避することができます。*プロキシCA証明書をインポート*をクリックすると、ユーザのブラウザに、他の目的に対してCAを信頼するか確認するプロンプトが表示されます。詳しくは、*Webプロテクション* > *フィルタオプション* > *HTTPS CA*の章を参照してください。

- ログアウト: ユーザポータルからログアウトするには、ここをクリックします。これは、ログイン時に*ログインを記憶*を選択した場合に（これによりクッキーが作成されます）、明示的にログアウトしてこのクッキーを削除したいときのみ必要です。そうでない場合は、この *ログアウト*リ

ンクを使用する必要はありません。ブラウザのタブまたはウインドウを閉じるだけで十分です。

4.6.1 グローバル

マネジメント > *ユーザポータル* > *グローバル*タブで、ユーザポータルを有効化できます。さらに、ユーザポータルへのアクセスを許可するネットワークとユーザを指定できます。

ユーザポータルへのアクセスを有効にするには、以下の手順に従います。

1. **ユーザポータルを有効にします。**
   トグルスイッチをクリックします。

   ステータスアイコンがアンバー色に変わり*エンドユーザポータルオプション*エリアが編集可能になります。

2. **許可するネットワークを選択します。**
   ユーザポータルへのアクセスを許可するネットワークを追加または選択します。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

3. **許可するユーザを選択します。**
   ユーザポータルへのアクセスを許可するユーザまたはユーザグループを選択または新規追加します。ユーザを追加する方法は、*定義とユーザ* > *ユーザとグループ* > *ユーザ*ページで説明しています。

   すべてのユーザにアクセスを許可しない場合は、*許可されたすべてのユーザ*を選択解除し、ユーザとユーザグループを個々に選択します。

4. ***適用*をクリックします。**
   設定が保存されます。

   トグルスイッチが緑色に変わります。

4.6.2 詳細

*詳細*タブで、ユーザポータルの代替ホスト名とポート番号に加え、言語とセキュリティオプションを設定できます。

言語

ログイン時に、ユーザポータルはWebブラウザの言語設定をフェッチし、それぞれのロケールをロードして、ブラウザのデフォルトと同じ言語でポータルを表示します。ブラウザの言語設定がユーザ

ポータルで利用できない場合は、フォールバック（予備）の言語をここで選択できます。ユーザは、追加オプションとして、ユーザポータルのログインページで言語を選択できます。

セキュリティ

ユーザポータルはCookieを使用してセッションを追跡します。永続的（固定）Cookieにより、セッションを閉じた後で再度ログインしないで戻ることが可能になります。これらはいつでもユーザ側で削除できますが、ユーザポータルの*ログアウト*ボタンを使用することが必要です。

ポータル メニューの無効化

ここにリストされているそれぞれの機能をWebAdminで有効にすると、ユーザポータルにメニュー項目が表示されます。ただし、ここでは、ユーザポータルで表示*しない*メニュー項目を定義できます。これを定義するには、それぞれのオプションを選択して*適用*をクリックします。

ネットワーク設定

ホスト名：デフォルトでは、これが*マネジメント* > *システム設定* > *ホスト名*タブで与えられるUTMのホスト名です。ただし、インターネットを介してアクセスするユーザにユーザポータルへのアクセスを付与する場合は、パブリックに解決できる代替ホスト名をここに入力する必要があります。

リスンアドレス：デフォルトは*すべて*です。Webアプリケーションファイアウォールを使用する場合、サービスがユーザポータル接続をリスンするためのインタフェースアドレスを指定する必要があります。ユーザポータル接続ハンドラとWebアプリケーションファイアウォールが受信SSL接続を識別できるようにするために、この設定が必要です。

ポート：デフォルトでは、HTTPSのポート`443`が選択されています。ポートは、`1024`～`65535`の範囲内でどの値にでも変更できます。`10443`または*WebAdmin TCPポート*は選択できません。これは*マネジメント* > *WebAdmin設定* > *詳細*タブで設定されています。ユーザポータルは、定義したポートから独立しており、HTTPSのみを介して常にアクセスすることができます。

ウェルカムメッセージ

ユーザポータルのようこそメッセージをカスタマイズできます。シンプルなHTMLマークアップとハイパーリンクを使用できます。

注 – ホームユーザライセンスを使用している場合は、ようこそメッセージを変更できません。

4.7 通知

Sophos UTMには、UTMで発生するあらゆる種類のセキュリティ関連イベントについて、メールまたはSNMPトラップで即時通知する機能が搭載されています。管理者が知るべきすべてのイベントが、各種エラー、警告、情報コードによって示されます。どのような通知が送信されるのかは、*通知*タブで設定した選択内容に応じて決まります。

4.7.1 グローバル

マネジメント > *通知* > *グローバル*タブでは、が送信する通知Eメールに利用される送信者アドレス(つまり*送信元*アドレス)を設定できますUTM。デフォルトでは`do-not-reply@fw-notify.net`となっています。このアドレスを変更する場合、お客様のドメインのメールアドレスを入力することをお勧めします。この理由は、一部のメールサーバーでは、指定された送信者アドレスが本当に存在することを確認するように設定されているためです。

UTMさらに、通知の受信者を指定することができます。デフォルトでは、初期セットアップ時に入力された管理者のメールアドレスです。

通知を制限:一部のセキュリティ関連イベント(検出された侵入試行など)では、大量の通知が発生し、通知受信者の受信トレイが短時間でいっぱいになる可能性があります。このため、Sophos UTMには、1時間あたりに送信される通知数を制限するための妥当なデフォルト値が用意されています。このオプションを無効にすると、*マネジメント* > *通知* > *通知*タブで通知を送信するように設定されているすべてのセキュリティ関連のイベントから通知が発生します。

機器固有のテキスト

ここでは、Sophos UTMの説明(場所など)を入力できます。この情報は、送信される通知に示されます。

4.7.2 通知

通知は次の3つのカテゴリに分類されます。

- **CRIT**:UTMが操作不能になる可能性がある重大なイベントを通知するメッセージ。
- **WARN**:しきい値の超過など、ユーザの注意を必要とする潜在的な問題についての警告。
- **INFO**:システムコンポーネントの再起動など、情報提供目的のみのメッセージ。

通知をメールとSNMPトラップのいずれで送信するかを選択できます。

4.7.3 詳細

UTMでEメールを直接送信できない場合、Eメールを送信するスマートホストを設定することができます。次の手順で実行します。

1. *マネジメント* **>** *通知* **>** *詳細*タブで*外部SMTP*を有効にします。
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、*外部SMTPサーバ*エリアが編集可能になります。

2. **スマートホストを入力します。**
   ドラッグ&ドロップを使用できます。ポートは、デフォルトのSMTPポートである25に事前設定されています。

   - **TLSを使用**: 通知の送信でTLSを強制するには、このチェックボックスにチェックを入れます。スマートホストでTLSがサポートされない場合、通知は送信されません。

3. **認証の設定を指定します。**
   スマートホストで認証が必要な場合、*認証*チェックボックスにチェックを入れ、対応するユーザ名とパスワードを入力してください。

4. *適用*をクリックします。
   設定が保存されます。

   トグルスイッチが緑色に変わります。

4.8 カスタマイズ

*マネジメント > カスタマイズ*のタブを使用すると、Sophos UTMが生成するメール通知とステータスメッセージをカスタマイズおよびローカライズして、会社のポリシーやコーポレートアイデンティティに合わせてこれらのメッセージを調整することができます。

さらに、カスタムWebテンプレートを編集およびアップロードして、ユーザーがブロックメッセージやその他の通知を受信する方法をさらに変更することができます。

注 – ホームユーザーライセンスを使用している場合は、カスタマイズできません。

4.8.1 グローバル

*マネジメント > カスタマイズ > グローバル*タブでは、ユーザに表示されるシステムメッセージのグローバル表示オプションをカスタマイズすることができます。UTF-8/Unicodeがサポートされています。

ここでは、カスタマイズ可能なグローバルオプション(*会社ロゴ*および*カスタム会社テキスト*)や*マネジメント > カスタマイズ > Web メッセージ*ページで設定する「コンテンツのブロック」メッセージの例を示しています。
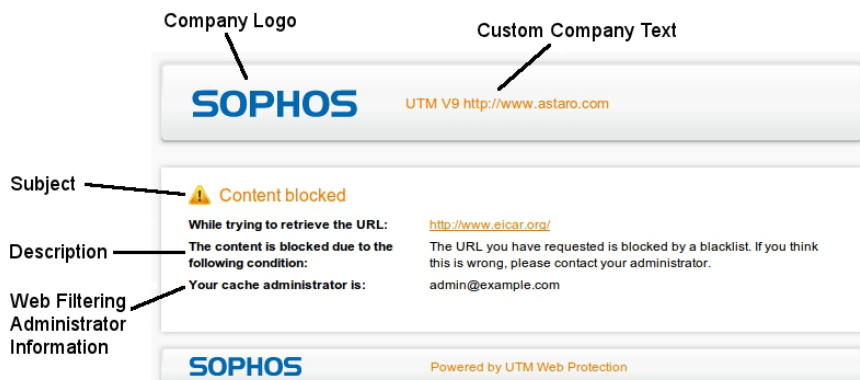
図 **12** カスタマイズ:ブロックされるページの例とカスタマイズ可能な部分

会社のロゴ

カンパニーロゴ/バナーをアップロードし(png 形式のみ)、次の状況で使用することができます。

- Webメッセージ
- 「ブロックされたPOP3メール」用メッセージ
- (隔離レポートを通じてスパムメールが隔離場所からリリースまたはホワイトリスト化された後で表示される)隔離リリースステータスメッセージ
- 隔離レポート

ユーザに表示されるメッセージの一部は、デフォルトのロゴ(195 x 73ピクセルで、背景が透明)に最適化されています。最もきれいに見える結果を得るには、同じ属性の画像を使用してください。

ロゴをアップロードするには:

1. *ファイルのアップロード***ダイアログボックスを開きます。**
   *新しいロゴのアップロード*ボックスの横にあるフォルダアイコンをクリックします。

   *ファイルのアップロード*ダイアログウィンドウが開きます。

2. **ロゴを選択します。**
   アップロードするロゴがある場所を参照します。

   ロゴを選択し、*アップロード開始*をクリックします。

3. ***適用*をクリックします。**
   ロゴがアップロードされ、すでにインストールされているファイルと置き換えられます。

カスタムカンパニーテキスト

Sophos UTMのウイルススキャナまたはコンテンツフィルタによってWebサイトがブロックされたときに、カンパニーロゴの下に表示されるメッセージをカスタマイズします。ここには、管理者の連絡先データなどを入力することができます。

4.8.2 Webメッセージ

Sophos UTMによって表示されるWebフィルタリングメッセージのテキストをカスタマイズします。一部のメッセージは、ファイルが大きすぎる、特定のタイプのファイルである、ウイルスを含んでいるなどの理由でファイルのダウンロードがユーザに対して制限された場合に表示されます。他のメッセージは、ファイルのダウンロード中にユーザが制限されているWebサイトやアプリケーションにアクセスしようとした場合、あるいはUTMによる認証が必要となった場合などに表示されます。これらのメッセージを他の言語に翻訳したり、たとえば、顧客サポートの連絡先情報などが表示されるように変更したりすることができます。

> **注 –** *Webメッセージ*タブのフィールドに入力されたテキストは、カスタムWebテンプレートで参照できます。詳細情報は、*Webテンプレート*を参照してください。

以下のメッセージを設定できます。

- *コンテンツのブロック*
  - *サーフプロテクション*: このメッセージは、ブロック対象として設定されているURLカテゴリと一致するコンテンツを持つWebページ、あるいはサイトの評判が指定されたしきい値を下回ったWebページにユーザがアクセスしようとすると表示されます。詳しくは、*Webプロテクション* > *Webフィルタリング*を参照してください。

- ブラックリスト: このメッセージは、ブラックリスト化されたのURLと一致するWebページをユーザが取得しようとすると表示されます。URLをブラックリスト化する方法は、*Webプロテクション > Webフィルタリング > ポリシ > Webサイトのフィルタリング*を参照してください。
- **MIME**タイプ: このメッセージは、ブロックされているMIMEタイプのファイルをユーザが要求すると表示されます。MIMEタイプの指定に関する詳細は、*Webプロテクション > Webフィルタリング > ポリシ > ダウンロード*を参照してください。
- ファイル拡張子: このメッセージは、ブロックされたファイル拡張子をユーザーが要求すると表示されます。ファイル拡張子の指定に関する詳細は、*Webプロテクション > Webフィルタリング > ポリシ > ダウンロード*を参照してください。
- ファイルサイズ: このメッセージは、ファイルサイズの上限を超えたファイルをユーザーが要求すると表示されます。ダウンロードサイズの限度を設定するには、*Webプロテクション > Webフィルタリング > ポリシ > ダウンロード*を参照してください。
- アプリケーション制御:このメッセージは、アプリケーション制御でブロックするように設定されている種類のネットワークトラフィックをユーザーが使用しようとした場合に表示されます。アプリケーション制御に関する詳細は、*Webプロテクション > アプリケーション制御*を参照してください。
- ウイルス検知: このメッセージは、ウイルス感染が原因でファイルがブロックされた場合に表示されます。ウイルス保護の設定に関する詳細は、*Webプロテクション > Webフィルタリング > ポリシ > ウイルス対策*を参照してください。

- ダウンロード/スキャン
  - ダウンロード進行中: このメッセージは、ファイルがダウンロードされている間、表示されます。*ダウンロードマネージャ*を参照してください。
  - ウイルススキャン実行中: このメッセージは、悪意あるコンテンツについてのUTMスキャンの間、表示されます。*ダウンロードマネージャ*を参照してください。
  - ダウンロード完了: このメッセージは、ファイルが完全にダウンロード、スキャン、安全と判断されると表示されます。*ダウンロードマネージャ*を参照してください。
- 認証
  - 透過モード認証: このオプションは、透過モードでWebフィルタリングを使用していて、"ブラウザ"認証モードを選択した場合にだけ適用されます。詳しくは、*Webプロテクション > Webフィルタプロファイル > フィルタプロファイル*を参照してください。テキストは認証ページに表示されます。各ユーザーはWebフィルタを使用する前にこの認証ページにログインする必要があります。*利用規約*フィールドが入力されていると、認証ページに免責条項が表示されます。このフィールドが空白(デフォルト)であれば、免責条項は表示されません。

- コンテンツブロックをバイパス: このメッセージは、ページがサーフプロテクションによってブロックされ、ブロックをバイパスするオプションが有効であると表示されます(*Web プロテクション* > *フィルタリングオプション* > *バイパスユーザ*を参照)。*利用規約*フィールドが入力されていると、認証ページに免責条項が表示されます。このフィールドが空白(デフォルト)であれば、免責条項は表示されません。
- エラー
    - サーバエラー: このメッセージは、ユーザからの要求の処理中にエラーが発生すると表示されます。
- 管理者情報: ここでは、管理者ののメールアドレスを含めて、Webフィルタを管理している管理者に関する情報を入力できます。

4.8.2.1 Web メッセージの変更

メッセージを変更するには、次の手順に従います。

1. **メッセージを選択します。**
   ページドロップダウンリストで、編集したいエンドユーザメッセージを選択します。

   そのメッセージの*件名*と*説明*が表示されます。

2. **件名および/または説明を変更します。**
   必要であれば、デフォルトテキストを変更します。

3. ***適用*をクリックします。**
   テキストの変更を保存します。

4.8.2.2 ダウンロードマネージャ

Webフィルタが有効である場合、サイズが1 MBを超え、コンテンツタイプがテキストまたは画像以外であるコンテンツのダウンロード中、Webブラウザに次のダウンロードページが表示されます。要求されているのが動画または音声ストリームである場合や、5秒以内にファイルの 50% 超のダウンロードが完了している場合には、ダウンロードページは表示されません。

ダウンロードページで提供される情報は、*Web メッセージ*タブでカスタマイズできます。
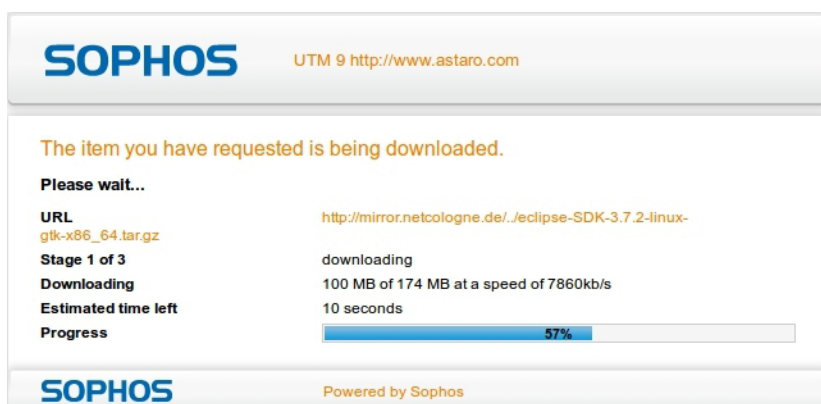
図 **13** カスタマイズ:HTTPダウンロードページ、ステップ1/3:ファイルのダウンロード
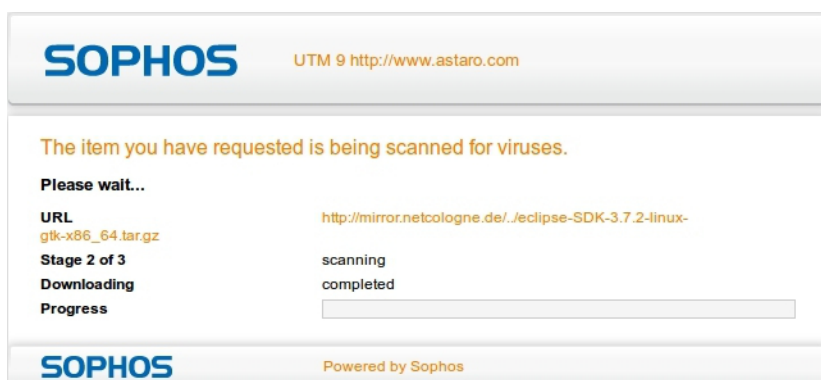
図 **14** カスタマイズ:HTTPダウンロードページ、ステップ2/3:ウイルススキャン
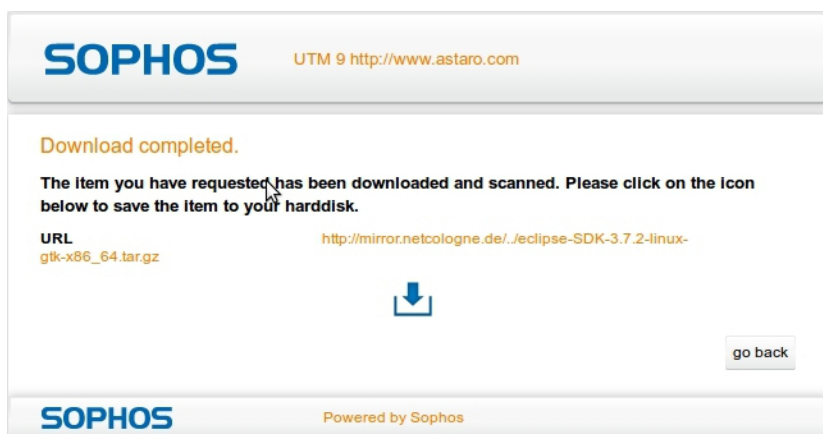
図 **15** カスタマイズ:HTTPダウンロードページ、ステップ3/3:ファイルのダウンロード完了

4.8.3 Webテンプレート

ユーザに表示されるメッセージの外観と内容の両方をカスタマイズするには、HTMLファイルをSophos UTMへアップロードします。ガイドとして、Sophosはいくつかのサンプルテンプレートを提供しています。こうしたテンプレートは、個別のユーザメッセージに関連する情報を動的に挿入できる変数の使用方法を示しています。たとえば、ウイルスを含むためあるファイルがブロックされたとすると、そのブロックされたウイルスの名前を挿入する変数を含めることができます。

4.8.3.1 Webテンプレートのカスタマイズ

警告 – Sophos UTM通知のカスタマイズは高度なトピックです。こうしたタスクを試みることができるのは、HTMLやJavaScriptの知識が十分にあるユーザだけです。

ブロックメッセージ、ステータスメッセージ、エラーメッセージ、認証プロンプトを含めて、カスタムバージョンのSophos UTM通知をアップロードすることができます。4つのサンプルテンプレートは、変数の動作例ならびにいくつかのサンプル画像を含んでいます。サンプルテンプレートをカスタムメッセージのベースとして使用するか、あるいは独自のHTMLファイルをアップロードしてください。有効な変数については、Sophos KnowledgebaseのUTM Webテンプレートでの変数の使用に説明があります。

*Webメッセージ*タブで設定したメッセージからのテキストを使用したい場合は、該当する変数をカスタムテンプレートに挿入することができます。詳細情報は、*Webメッセージ*を参照してください。

サンプルテンプレートおよび画像をダウンロードするには、下のリンクをクリックして、.zip ファイルを保存してください。

http://www.astaro.com/lists/Web_Templates.zip

4.8.3.2 カスタムWebテンプレートおよび画像のアップロード

カスタムテンプレートの編集、保存が完了すると、UTMへのアップロードの準備完了です。

Webテンプレートまたは画像をアップロードするには:

1. ***ファイルのアップロード*ダイアログボックスを開きます。**
   アップロードしたいテンプレートのタイプの名前の横にあるフォルダアイコンをクリックするか、画像をアップロードしたいのであれば、*画像*の横にあるフォルダアイコンをクリックします。

   > 注 – サポートされているファイルのタイプは、`.png`、`.jpg`、`.jpeg`、`.gif`です。

   *ファイルのアップロード*ダイアログウィンドウが開きます。

2. **テンプレートまたは画像を選択します。**
   アップロードしたいテンプレートまたは画像の場所を参照します。

   テンプレートまたは画像を選択し、*アップロード開始*をクリックします。

   *ファイルのアップロード*ダイアログウィンドウが閉じます。

3. ***適用*をクリックします。**
   テンプレートまたは画像がアップロードされます。

4.8.4 メールメッセージ

Sophos UTMの SMTP/POP3プロキシによって生成されるユーザーメッセージに表示されるテキストをカスタマイズします。これらのメッセージを他の言語に翻訳したり、顧客サポートの連絡先情報が表示されるように変更したりできます。次のメッセージをカスタマイズできます。

隔離

隔離からリリースされたメール:このメッセージは、メールが隔離から正常にリリースされたときに表示されます。

隔離からメールをリリースする際にエラー:このメッセージは、メールを隔離からリリースする際にエラーが発生したときに表示されます。

POP3

ブロックされた**POP3** メッセージ:このメッセージは、POP3メールのメッセージがブロックされたときに受信者に送信されます。
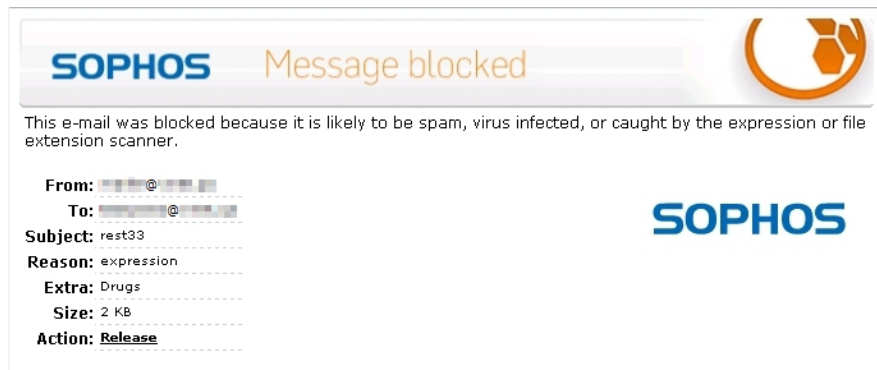
図 **16** カスタマイズ:POP3プロキシのブロックメッセージ

SPX

SPX 暗号化が有効化され、間違いが起こった際、これらの通知メールが送信されます。通知は指定された人物に送信されます(*メール暗号化* > *SPX暗号化* > *SPX設定* タブを参照)。

送信者指定パスワードが不明:このメールは、送信者がSPX暗号化用パスワードを指定していない場合、指定された人物に送信されます。

送信者指定パスワードが短すぎる:このメールは、メール送信者が指定したパスワードが短すぎる場合に指定された人物に送信されます。

送信者指定パスワードが特殊文字を含んでいない:このメールは、メール送信者が指定したパスワードに必要な特殊文字が含まれていない場合に指定された人物に送信されます。

内部エラー:このメールは、技術的な問題によりメールが送信されなかった場合に指定された人物に送信されます。

内部エラー - 送信者通知:このメールは、SPXメールの作成中のエラーによりメールが送信されなかった場合に指定された人物に送信されます。

返信ポータル**URL**が見つからない:このメッセージは、*受信者が返信*ボタンをクリックし、下位のURL が見つからなかった場合に返信ポータルページに表示されます。

デフォルト設定では、通知に使用することができる一部の変数が表示されます:

- %%送信者%%(メールの件名のみ):メール送信者
- %%受信者%%:メール受信者
- %%理由%%(メールの説明のみ):メッセージの理由。適切なエラーテキストに置換されます。

4.9 SNMP

簡易ネットワーク管理プロトコル(SNMP)は、ルータ、サーバ、スイッチなどのネットワークに接続されたデバイスを監視するためにネットワーク管理システムで使用されます。SNMPによって管理者は、監視している各ネットワークデバイスの状態に関するクエリを速やかに実行できます。Sophos UTMは、SNMP クエリに返答したり、SNMP トラップを SNMP 管理ツールに送信するように設定できます。前者は「*管理情報ベース(MIB)*」によって実現します。MIBは、どのネットワークデバイスに対してどの情報がクエリ可能かを指定します。Sophos UTMは、SNMPバージョン2と3および以下のMIBをサポートしています。

- **DISMAN-EVENT-MIB**:イベント管理情報ベース
- **HOST-RESOURCES-MIB**:ホストリソース管理情報ベース
- **IF-MIB**:インタフェースグループ管理情報ベース
- **IP-FORWARD-MIB**:IPフォワーディングテーブル管理情報ベース
- **IP-MIB**:*インターネットプロトコル*(IP)用管理情報ベース
- **NOTIFICATION-LOG-MIB**:通知ログ管理情報ベース
- **RFC1213-MIB**:TCP/IPベースのインターネットのネットワーク管理用管理情報ベース:MIB II
- **SNMPv2-MIB**:*簡易ネットワーク管理プロトコル*(SNMP)用管理情報ベース
- **TCP-MIB**:*伝送制御プロトコル*(TCP)用管理情報ベース
- **UDP-MIB**:*ユーザデータグラムプロトコル*(UDP)用管理情報ベース

Sophos UTMシステム情報を取得するには、最低でもRFC1213-MIB (MIB II)をコンパイルしたSNMP マネージャを使用する必要があります。

4.9.1 クエリ

*マネジメント > SNMP > クエリ*ページでは、SNMPクエリの使用を有効にできます。

SNMPクエリを設定するには、次の手順に従ってください。

1. ***SNMPクエリ*を有効にします。**
   トグルスイッチをクリックします。

   *SNMPバージョン*および*SNMPアクセスコントロール*セクションが編集可能になります。

2. **SNMPバージョンを選択します。**
   *SNMPバージョン*セクションで、ドロップダウンリストからバージョンを選択します。SNMPバージョン3には認証が必要です。

3. **許可されるネットワークを選択します。**
   *許可ネットワーク*ボックスにリストされているネットワークは、Sophos UTM上で実行されているSNMPエージェントにクエリを行うことができます。アクセスは常に読み取り専用です。

   - コミュニティ名：バージョン2を使用する場合、コミュニティ名を入力します。SNMPコミュニティ名はパスワードとして機能し、SNMPエージェントへのアクセスを保護します。デフォルトでは、SNMPコミュニティ名は"public"に設定されていますが、お客様のニーズに応じて変更できます。

     注 – コミュニティ名に使用できる文字：(a～z)、(A～Z)、(0～9)、(+)、(_)、(@)、(.)、(-)、(空白)

   - ユーザ名/パスワード：バージョン3を使用する場合、認証が必要です。ユーザ名とパスワード（確認のために2回）を入力し、リモート管理者がクエリを送信できるようにします。パスワードは8文字以上にする必要があります。SNMP v3では、認証にSHAを、暗号化にAESを使用します。ユーザ名とパスワードはその両方で使用されます。

4. ***適用*をクリックします。**
   設定が保存されます。

さらに、UTMについての追加情報を入力できます。

デバイス情報

*デバイス情報*テキストボックスに、名前、場所、管理者など、UTMに関する追加情報を指定できます。この情報は、SNMP 管理ツールが読み取って、UTMの識別に使用します。

注 – UTM と*許可ネットワーク*間のすべてのSNMPトラフィック（プロトコルバージョン2）は暗号化されず、パブリックネットワーク上での転送中に読むことができます。

Astaro Notifier MIB

Sophos UTMこのセクションで、通知SNMPトラップの定義を含むAstaro MIBのダウンロードを行うことができます。歴史的な理由により、MIB はAstaroの私企業コードを使用します(SNMPv2-SMI::enterprises.astaro)。

4.9.2 トラップ

*トラップ*タブで、UTMで発生した関連イベントの通知をSNMPトラップとして送信する宛先のSNMPトラップサーバを定義できます。これらのトラップを表示するには、特別なSNMPモニタリングソフトウェアが必要です。

SNMPトラップとして送られるメッセージには、オブジェクト識別子(OID)が含まれます。たとえば、`.1.3.6.1.4.1.9789`が挙げられます。これは、IANAが発行した私企業番号に属します。`.1.3.6.1.4.1`は`iso.org.dod.internet.private.enterprise`プレフィックスで、`9789`はAstaroの*私企業番号*です。通知イベントのOIDは`1500`で、それに通知タイプのOIDおよび対応するエラーコード(`000-999`)が追加されます。以下の通知タイプを使用できます。

- `DEBUG = 0`
- `INFO = 1`
- `WARN = 2`
- `CRIT = 3`

例:通知「INFO-302:新しいファームウェアUp2Dateがインストールされました(New firmware Up2Date installed)」では、OID `.1.3.6.1.4.1.9789.1500.1.302`を使用し、以下の文字列が割り当てられます。

```
[<HOST>][INFO][302]
```

`<HOST>` はシステムのホスト名を表わすプレースホルダであり、通知の件名フィールドのタイプおよびエラーコードのみが伝送されます。

SNMP v2cトラップサーバを選択するには、以下の手順に従います。

1. ***新規SNMPトラップシンク*をクリックします。**
   *SNMPトラップシンクの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   SNMPバージョン:ドロップダウンリストから*SNMP v2c*を選択します。

   ホスト: SNMPトラップサーバのホスト定義。

コミュニティ: SNMPコミュニティ名はパスワードとして機能し、クエリを行うSNMPメッセージへのアクセスを保護します。デフォルトでは、SNMPコミュニティ名は"public"に設定されています。それをリモートSNMPトラップサーバで設定された文字列に変更します。

> **注 -** コミュニティ名に使用できる文字 : (a～z)、(A～Z)、(0～9)、(+)、(_)、(@)、(.)、(-)、(空白)

コメント(オプション) : 説明などの情報を追加します。

3. ***保存*をクリックします。**
   新しいSNMPトラップサーバが *トラップ*タブに表示されます。

SNMPバージョン3には認証が必要です。SNMP v3トラップサーバを選択するには、以下の手順に従います。

1. ***新規 SNMP トラップシンク*をクリックします。**
   *新規 SNMP トラップシンクの作成*ダイアログボックスが開きます。
2. **次の設定を行います。**
   SNMPバージョン: ドロップダウンリストから*SNMP v3*を選択します。

   ホスト: SNMPトラップサーバのホスト定義。

   ユーザ名 : 認証のユーザ名を入力します。

   認証 タイプ: ドロップダウンリストから認証のタイプを選択します。

   パスワード: 認証のパスワードを入力します。

   再入力 : 認証のパスワードを再入力します。

   暗号化 タイプ: ドロップダウンリストから暗号化のタイプを選択します。

   パスワード: 暗号化のパスワードを入力します。

   再入力 : 暗号化のパスワードを再入力します。

   エンジン**ID** : エンジンのIDを入力します。

   コメント(オプション) : 説明などの情報を追加します。
3. ***保存*をクリックします。**
   新しいSNMPトラップサーバが *トラップ*タブに表示されます。

4.10 集中管理(SUM)

*集中管理(SUM)*メニューのページを使用すると、ゲートウェイのモニタリングやリモート管理に使用できる管理ツールへのインタフェースを設定することができます。

4.10.1 Sophos UTM Manager

Sophos UTM Manager(SUM)は、Sophosの一元(集中)管理用製品です。複数のUTMアプライアンスをSUMに接続して、一元的にモニタリング、設定、メンテナンスができます。SUM 4.2は、UTM9.2の設定のみサポートします。その他のUTMバージョンは、SUMに表示され、また監視されます。例えばUTM9.2がSUM 4.1と接続している場合、レガシーモードに入ります。その際、バックアップおよびup2dateのインストールが可能な状態です。

このタブでは、UTMを1つまたは2つのSUMへ接続する際の設定ができます。

注 – MSPライセンスを使用する場合、SUMの無効化、SUMホストの変更、SUM管理者の権限の変更は、SophosUTM Manager(SUM)でのみ実行できます。

Sophos UTMがSUMサーバーのモニタリング対象とされるよう準備するには、次の手順に従ってください。

1. ***Sophos UTM マネージャタブで、SUMを有効にします。***
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、*SUM 設定*エリアが編集可能になります。

2. ***SUM ホスト*を指定します。**
   接続先とするSUMサーバのUTMを選択または追加します。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

   - 認証(オプション):SUMサーバで認証が必要な場合、このオプションを選択して、SUMサーバで設定したものと同じパスワード(共有シークレット)を入力します。

   - **Up2DateキャッシュとしてSUMサーバを使用します**(オプション):Up2Dateパッケージは、SUMサーバにあるキャッシュから取得することができます。ゲートウェイ用にこの機能を使用するには、*SUM サーバーをUp2Date キャッシュとして使用*オプションを選択します。管理している SUM サーバーで、Up2Date キャッシュ機能を適切に有効にしていることを確認してください。Up2Date キャッシュは、UpDates の親プロキシ設定と同時に使用できないことに注意してください。

3. **SUM の管理者の権限を定義します。**
SUM で管理者は、管理を許された UTM の特定のエリアのみ管理することができます。ここでリストされている権限は、SUM ゲートウェイマネージャのメインメニューおよび権限オプションと一致します。

管理 : これを選択すると、管理者は *メンテナンス*および *マネジメント*メニューに用意されたすべての機能を使用できます。たとえば、リストの表示、バックアップの作成とリストア、ファームウェアアップデートのスケジュール設定などです。

レポーティング: これを選択すると、管理者は *レポーティング*メニューに用意されたすべての機能を使用できます。たとえば、UTM からレポートを要求できます。

モニタリング: これを選択すると、UTMが *モニタリング*ページに表示され、管理者はすべての関連機能を使用できます。

設定 : これを選択すると、管理者は*設定*メニューに用意されたすべての機能を使用できます。たとえば、ネットワーク、ホスト、VPN などのオブジェクトを UTM にデプロイできます。

注 – 詳細は、Sophos UTMマネージャ管理ガイドを参照してください。

4. ***適用*をクリックします。**
設定が保存されます。

トグルスイッチが緑色に変わります。

UTMは、ここでSophos UTMマネージャへの接続を確立しようとします。両システム間の接続が確立したら、接続ステータスは緑色に変わります。ここで選択するSUMサーバによって、UTMをモニタリングおよび管理できるようになります。*SUMのステータス*セクションで、現在の接続のステータスと健全性を確認することができます。ページをリロードすると、このデータが更新されます。接続に関する問題が発生した場合は、*ライブログを開く*ボタンを使用し、掲示板のメッセージを参照して問題を診断してください。

2台目のSUMの設定

このセクションでは、2台目のSUMを任意に追加することができます。これは、例えばご自分で設定を行い(1台目のSUMサーバー)、かつ第三者、例えばMSSPによるモニタを必要とする場合(2台目のSUMサーバー)などに有効です。この設定は1台目のSUMサーバーとほぼ同様です。ただし、*設定*のオプションは1台目のSUMサーバーに限られているため、2台目では設定できません。

注 – ゲートウェイとSUMの間の通信はポート4433で行われますが、Sophos UTM Managerには、HTTPSプロトコルを使用してブラウザ経由でアクセスすることができます。WebAdminの場合はポート4444、ゲートウェイマネージャインタフェースの場合はポート4422です。

SUMのステータス

*SUM のステータス*セクションで、現在の接続ステータスと健全性を確認することができます。ページをリロードすると、このデータが更新されます。

SUMオブジェクト

このエリアは、SUM経由で作成されたオブジェクトがあり、このSUMがSophos UTMから切断されている場合を除き、無効になっています(グレーアウト表示されています)。SUMで作成されたオブジェクトとは、ネットワーク定義、リモートホスト定義、IPsec VPNトンネルなどです。

*オブジェクトのクリーンアップ*ボタンを押すと、デバイスを以前に管理していたSUMで作成されたすべてのオブジェクトをリリースすることができます。これらのオブジェクトは通常ロックされ、ローカルデバイスのみで表示できます。このボタンを押すと、オブジェクトは完全にアクセス可能になり、ローカル管理者が再利用または削除できます。使用されていないオブジェクトがある場合、それらは直接削除され再利用されません。

注 – 以前に SUM で作成されたオブジェクトをクリーンアップすると、同じ SUM に再接続したときにこれらのオブジェクトを再変換できなくなります。つまりリモートのSUMが、後で接続を再確立するデバイス用にオブジェクト定義をまだホストしている場合、ローカルコピーがすでに存在しても、これらのオブジェクトはデバイスに再配備されます。

ライブログ

ライブログを使用して、Sophos UTMとSUMの間の接続をモニタリングすることができます。クリック *ライブログ*ライブログを新しいウインドウで開くためのボタン。

4.11 Sophos Mobile Control (SMC)

Sophos Mobile Control (SMC) により、iOS、AndroidまたはWindows Phone搭載のスマートフォンやタブレットといった、会社のEメールモバイルデバイスのインストール/特定/セキュアが許可されているアプリを、管理/セキュア/アップデート/制御できます。Sophos Mobile Control WebAdminインタフェースを利用して、対応デバイスおよびユーザの定義、ネットワークアクセス制御の設定、および設定のSMCサーバへのプッシュができます。

さらなる詳細については、Sophos Mobile Control Webサイトをご覧ください。

SMCサーバ

SMCは別のサーバ上で実行されます。Sophos UTMでは、SMCサーバを接続して、対応/非対応のデバイスおよびユーザの概要の取得、VPNおよびワイヤレスネットワークのネットワークアクセスの定義、ネットワーク設定のSMCサーバへののプッシュが行えます。

SMCサーバは、2つの異なる方法で実行できます。

- 施設内インストールでは、お持ちのサーバ上へとデータを社内保管できます。
- SMCをサービスバージョンとして利用すると、お客様の側でハードウェアを用意する必要がありません。

注 – SMCを利用するには、有効なライセンスが必要です。Sophos Mobile Control Webサイトからソフトウェアをダウンロードすると、トライアルライセンスが送付されます。フルライセンスは、最寄りのSophosパートナーから入手可能です。

SMCサーバおよびライセンスについてのさらなる情報は、Sophos Mobile Controlマニュアルでご確認ください。

SMCアプリ

モバイルデバイス上でSMCを使用するには、SMCアプリをスマートフォンまたはタブレットにダウンロードする必要があります。アプリは無料で、各アプリストア（Apple iTunes、Google Play、またはWindows App Store）でダウンロード可能です。

- iOS向けiTunesでSMCアプリをダウンロードする
- Android向けGoogle PlayでSMCアプリをダウンロードする
- Windows Phone向けWindows App StoreでSMCアプリをダウンロードする

4.11.1 一般

*マネジメント > Sophos Mobile Control > 一般*タブでは、Sophos Mobile Controlのホストを定義できるほか、顧客の詳細およびSMCサーバのログイン資格情報を指定できます。SMC管理者が顧客アカウントおよびログインデータを作成します。

注 – このタブ上ではSMCサーバの作成はできません。SMCサーバの作成についてのさらなる情報は、Sophos Mobile Controlマニュアルでご確認ください。

1. **Sophos Mobile Controlの有効化:**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、*グローバル設定*エリアが編集可能になります。

2. **次の設定を行います。**
   SMC サーバ: サーバをホストSMCへと追加または選択します。

   顧客: SMC顧客を入力します。

   ユーザ名: SMCユーザ名を入力します。

   パスワード: SMCパスワードを入力します。

   注 – Sophos UTM内で新規顧客の作成、ユーザまたはパスワードの定義はできません。新規顧客は直接、SMC内でのみ作成可能です。

   CA証明書: 公式のWeb CAまたはカスタムの認証局を選択します。*サイト間VPN* > *証明書管理* > *認証局*タブで、ユニットに新しい認証局を追加できます。

3. *情報*ダイアログウィンドウが開きます。
   - 接続テスト成功: SMCサーバへの接続が成功しました。
   - 接続テスト失敗: SMCサーバへの接続に失敗しました。

   注 - SMCサーバへの接続に失敗した場合、Sophos Mobile Controlライブログを利用して、問題を見つけ出します。

4. **次の詳細設定を任意で行います。**
   デバッグモードの有効化: このオプションで、Sophos Mobile Controlログで生成されるデバッグ出力の量を制御します。接続で問題が発生した場合や、クライアントパラメータのネゴシエーションに関する詳細な情報が必要である場合などに、このオプションを選択します。

5. ***適用*をクリックします。**
   設定が保存されます。

   トグルスイッチが緑色に変わります。

ライブログを開く

Sophos Mobile Controlライブログは、Sophos Mobile Controlインタフェース上の全アクティビティをロギングします。*ライブログを開く*ボタンをクリックすると、新しいウィンドウでSophos Mobile Controlライブログが開きます。

4.11.2 コンプライアンスの概要

*マネジメント > Sophos Mobile Control > コンプライアンスの概要*タブには、Sophos UTMに接続されている全モバイルデバイスがリストされています。SMCサーバは、モバイルデバイスまたはユーザの接続を許可する、特定のポリシを設定します。モバイルデバイスまたはユーザがポリシに対応していない場合、それらは非対応デバイス/ユーザとしてブラックリストにリストされます。ポリシに非対応である原因は、例えば、デバイスに適切なプラットフォームがない、または許可されていない特定のアプリを使用している場合が考えられます。対応デバイスはホワイトリストに表示されます。

- *非対応デバイス*: ワイヤレスネットワークのブラックリスト上のすべての非対応デバイスのMACアドレスです。
- *対応デバイス*: ワイヤレスネットワークのホワイトリスト上のすべての対応デバイスのMACアドレスです。
- *非対応ユーザ*: VPNブラックリストに記載されている非対応ユーザの名前です。

4.11.3 ネットワークアクセスコントロール

*マネジメント > Sophos Mobile Control > ネットワークアクセスコントロール*タブでは、VPN接続およびワイヤレスネットワークのアクセス設定を設定できます。定義済みのVPNまたはワイヤレスネットワークに向かう非対応デバイスは、ブロックされます。

特定のVPNネットワークへのアクセスをブロックする

会社ポリシに非対応のモバイルデバイスを使用するユーザをブロックするよう、VPNおよびワイヤレスネットワークを定義します。

- **L2TP over IPsecを施行**: 選択すると、非対応ユーザはL2TP over IPsec経由でSophos Mobile Controlに接続できなくなります。
- **Cisco™ VPNを施行**: 選択すると、非対応ユーザはCisco™ VPN経由でSophos Mobile Controlに接続できなくなります。

- 他のVPNプロトコルに対するアクセスも拒否：選択すると、非対応ユーザはその他のVPNプロトコル経由でSophos Mobile Controlに接続できなくなります。

ワイヤレスネットワークを施行：これらのワイヤレスネットワーク経由でSophos Mobile Controlに接続しようとする非対応デバイスをブロックします。

対応状態のポーリング：現在の対応状態がSMCサーバからポーリングされる間隔を分（1～60）で入力します。

4.11.4 構成設定

マネジメント > *Sophos Mobile Control* > *設定*タブでは、WebAdminからのVPNおよびワイヤレスネットワーク設定をSMCサーバへとプッシュできます。これらの設定により、モバイルデバイスおよびユーザのUTMへの接続方法が定義されます。設定はSMCから、接続されたモバイルデバイスへと送信されます。VPNおよびワイヤレスネットワーク設定を、手動で設定する必要はありません。

Sophos Mobile Controlの構成設定

どのVPNおよびワイヤレスネットワーク設定を、SMCサーバへとプッシュするか定義します。

- **L2TP over IPsec**設定：選択すると、L2TP over IPsec設定がSMCサーバへとプッシュされます。
- **Cisco™ VPN**設定：選択すると、Cisco™ VPN設定がSMCサーバへとプッシュされます。

ワイヤレスネットワーク：SMCサーバへとプッシュするワイヤレスネットワークを選択します。

EAP メソッド：ワイヤレスネットワークエンタープライズ認証を使用するEAPメソッド（拡張認証プロトコル）を選択します。

設定のプッシュ

現在の設定をSMCサーバへと転送するには、*今すぐ設定をプッシュ*ボタンをクリックします。

注 – 例えば送信中にサーバがオフラインであったというような例外的なケースでのみ、この機能を使用してください。通常、このボタンを使用して設定をプッシュする必要はありません。

4.12 冗長化(HA)

インターネットセキュリティシステムの障害の主な原因は、ハードウェアの故障です。システムに障害が発生した後もサービスを継続して提供する能力をフェイルオーバーと呼びます。Sophos UTM

はHAフェイルオーバーを実現するため、お客様はプライマリシステムで障害が発生したときのためにホットスタンバイシステムをセットアップできます(active-passive)。あるいは、Sophos UTMを使用してクラスタをセットアップして、専用のネットワークトラフィックを一群のノードに分散させて運用し(active-active)、リソース利用率を最大限に高めて処理時間を削減することができます。これは従来のロードバランシングアプローチと似ています。

Sophos UTMに導入された*冗長化*と*クラスタ*の概念は、緊密に連携しています。HAシステムは2ノードクラスタと考えることができます。これは冗長性を実現する最低限の要件です。

これは冗長性を実現する最低限の要件です。

- マスタ: ホットスタンバイ/クラスタセットアップ内のプライマリシステム。クラスタ内で、マスタはデータの同期と配信を行う責任を担います。
- スレーブ: ホットスタンバイ/クラスタセットアップ内のスタンバイシステム。マスタに障害が発生すると、オペレーションを引き継ぎます(テイクオーバーします)。
- ワーカ: データ処理のみを担当するシンプルなクラスタノード。

すべてのノードは、いわゆるハートビート信号を使用して自らをモニタリングします。ハートビート信号とは、他のノードが稼働していることを確認するために定期的に送信されるマルチキャストUDPパケットです。技術的エラーが原因で、いずれかのノードがこのパケットの送信に失敗すると、そのノードは*デッド*と宣言されます。失敗したノードが担っていた役割に応じて、セットアップの構成が次のように変更されます。

- マスタノードで障害が発生した場合、スレーブがマスタの役割を引き継ぎ、IDが最も高いワーカノードがスレーブとなります。
- スレーブノードで障害が発生した場合、IDが最も高いワーカノードがスレーブとなります。
- ワーカノードで障害が発生した場合、処理能力が失われることによるパフォーマンス低下は認識されますが、フェイルオーバー機能は損なわれません。

注 – HA設定はハードウェア設定の一部であり、バックアップには保存できません。これは、HA設定はバックアップリストアにより上書きされないということも意味します。

レポーティング

すべてのレポーティングデータはマスタノード上で統合され、5分間隔で他のクラスタノードと同期されます。したがって、引き継ぎが発生すると、最大過去5分間のレポーティングデータが失われます。ただし、データ収集プロセスには違いがあります。*ログとレポート > ハードウェア*タブに表示されるグラフには、現在マスタとなっているノードのデータのみが表示されます。*ログとレポート > ハードウェア*タブに表示されるグラフには、現在マスタとなっているノードのデータのみが表示されます。

たとえば、今日のCPU使用状況のヒストグラムには、マスタノードの現在のプロセッサ使用状況が表示されます。切り替わりが発生した場合、ここにはスレーブノードのデータが表示されるようになります。一方、上位アカウンティングサービスに関する情報などは、ユニットを通過するトラフィックの分散処理に関与したすべてのノードから収集されたデータの集合体となります。

注記

- *アドレス解決プロトコル*(ARP)を使用するのは、実際のマスタのみです。つまり、スレーブノードとワーカノードはARP要求の送信や応答を行いません。
- フェイルオーバーが発生すると、オペレーションを引き継ぐユニットがARPアナウンスメント(別名*gratuitous ARP*)を実行します。これは通常、要求を受信する他のホストのARPキャッシュを更新することを目的とするARP要求です。Gratuitous ARPは、マスタのIPがスレーブに移行したことをアナウンスするために使用されます。
- マスタで設定するすべてのインタフェースには物理リンクが必要です。つまり、任意のネットワークデバイスにポートを正しく接続しなければなりません。

4.12.1 ハードウェアとソフトウェアの要件

HAフェイルオーバーまたはクラスタ機能を提供するためには、次のハードウェアおよびソフトウェア要件を満たす必要があります。

- 冗長化オプションが使用可能な有効なライセンス(スタンバイユニットの場合、追加の基本ライセンスのみが必要です)。
- ソフトウェアバージョンとハードウェアが同じである2台のUTMユニット、または同じモデルの2台のUTMアプライアンス。
- ハートビートが可能なイーサネットネットワークカード。サポートされているネットワークカードを確認するには、HCL をチェックしてください。HCLはSophos Knowledgebaseで提供されています(検索用語に「HCL」を使用します)。
- イーサネットクロスオーバーケーブル(ホットスタンバイシステムでのマスタとスレーブの接続用)。UTM専用HAインタフェースがギガビット自動MDXデバイスである アプライアンスのモデル320、425、525は、標準のIEEE 802.3イーサネットケーブルで接続可能です(イーサネットポートが送信/受信ペアを自動的に交換するため)。
- ネットワークスイッチ(クラスタノードの接続用)。

4.12.2 ステータス

*マネジメント > 冗長化 > ステータス*タブには、ホットスタンバイシステムまたはクラスタに関与するすべてのデバイスがリストされ、次の情報が表示されます。

- **ID**: デバイスのノードID。ホットスタンバイシステムでは、ノードIDは1または2です。

  クラスタ内のノードIDは1～10の範囲になります。この理由は、1つのクラスタに最大10ノードまで持たせることができるためです。

- 役割: HAシステムは2ノードクラスタと考えることができます。これは冗長性を実現する最低限の要件です。
  - MASTER: ホットスタンバイ/クラスタセットアップ上のプライマリシステム。クラスタ内でデータの同期と配信を行う責任を担います。
  - SLAVE: ホットスタンバイ/クラスタセットアップ内のスタンバイシステム。マスタに障害が発生すると、オペレーションを引き継ぎます(テイクオーバーします)。
  - WORKER: データ処理のみを担当するシンプルなクラスタノード。
- デバイス名: デバイスの名前です。
- *ステータス*: HAステータスに関するデバイスの状態。次のいずれかになります。
  - ACTIVE: ノードは完全に機能しています。ホットスタンバイ(アクティブ-パッシブ)設定の場合、これがアクティブノードのステータスです。
  - READY: ノードは完全に操作可能です。ホットスタンバイ(アクティブ-パッシブ)設定の場合、これがパッシブノードのステータスです。
  - RESERVED: ノードに一致するバージョンがなく、プロセスに関与していません。
  - UNLINKED: 1つ以上のインタフェースリンクがダウンしています。
  - UP2DATE: Up2Dateが進行中です。
  - UP2DATE-FAILED: Up2Dateが失敗しました。
  - DEAD: ノードに到達できません。
  - SYNCING: データ同期が進行中です。このステータスは、ノードがマスタに接続しているときに表示されます。最初の同期には5分以上時間がかかります。あらゆる同期関連のプログラムにより、この時間が長期化する場合もあります。スレーブが同期中であり*同期中*ステータスの場合、マスタノードでのリンク障害などが原因で正常な引き継ぎは行われません。

- バージョン: Sophos UTM システムにインストールされたソフトウェアのバージョン番号。
- 最後のステータス変化: ステータス変更が最後に発生した時間。

リブート/シャットダウン: これらのボタンを使用して、デバイスを手動でリブートまたはシャットダウンすることができます。

ノード削除: このボタンを使用して、WebAdmin経由でデッド状態のクラスタノードを削除します。メール隔離やスプールなど、ノード固有のすべてのデータがマスタに引き継がれます。

HAライブログを別ウィンドウで表示するには、右上隅にある*HA ライブログを開く*ボタンをクリックします。

4.12.3 システムステータス

*マネジメント > 冗長化 > システムステータス*タブには、ホットスタンバイシステムまたはクラスタに関与するすべてのデバイスがリストされ、各デバイスのリソース使用状況に関する次の情報が表示されます。

- CPU 使用率(%)
- RAM 使用率(%) 表示される合計メモリは、オペレーティングシステムが使用できる部分であることに注意してください。32ビットシステムでは、一部がハードウェア用に予約されているため、必ずしも設置されている物理メモリの実際のサイズが表示されない場合もあります。
- スワップ使用状況(%)
- ログパーティションで消費されているハードディスクの容量(%)
- ルートパーティションで消費されているハードディスクの容量(%)
- UPS(無停電電源装置)モジュールがある場合はその状況

4.12.4 設定

Sophos UTMの冗長化機能は、4つのベーシック設定が可能です。

- オフ
- 自動設定
- ホットスタンバイ(アクティブ-パッシブ)
- クラスタ(アクティブ-アクティブ)

自動設定: Sophos UTMには、UTMアプライアンス用のプラグアンドプレイ設定オプションがあります。このオプションを使用すると、クラスタに追加するデバイスを再設定したり手動でインストールし

たりする必要なく、ホットスタンバイシステム/クラスタをセットアップすることができます。UTMアプライアンスの専用HAインタフェース(`eth3`)を相互に接続し、すべてのデバイスで*自動設定*を選択するだけで、準備は完了です。

> 注 – *自動設定*は、固定eth3ポート付きアプライアンスのデフォルトによってのみ有効化されます。モジュール型(リムーバブル)FlexiPortモジュールのみを提供するアプライアンスの場合、この機能はデフォルトにより無効となりますが、以下で説明するいずれかのポート(Sync NIC)上で有効とすることが可能です。

> 注 – *自動設定*が正常に機能するためには、すべてのUTMアプライアンスは同じモデルでなければなりません。たとえば、HAシステムのセットアップには、2台のUTM320アプライアンスを使用する必要があり、UTM220ユニットとUTM320ユニットを組み合わせて使用することはできません。

この専用インタフェースを介して2台のUTMアプライアンスを接続すると、すべてのデバイスが相互に認識し、HAシステムとして自動的に自己設定します。可能性は低いものの、アップタイムが同じであった場合には、MACアドレスに基づいてマスタとなるデバイスが決まります。

UTMソフトウェアを使用すると、専用スレーブシステムで*自動設定*オプションが使用され、マスタまたはすでに設定されているホットスタンバイシステム/クラスタに自動的に追加されます。このため、*自動設定*は、それ自体、冗長化オペレーションモードではなく移行モードと考えることができます。*自動設定*が選択されているデバイスがホットスタンバイシステムまたはクラスタに追加されると、冗長化オペレーションモードはそれぞれ*ホットスタンバイ*または*クラスタ*となります。ただし、この機能が正常に機能するためには、マスタシステムで*新規デバイスの自動設定を許可*オプションが有効になっていることが条件となります。この機能により、冗長化オペレーションモードが*自動設定*に設定されているデバイスがホットスタンバイシステム/クラスタに自動的に追加されます。

ホットスタンバイ **active-passive** :Sophos UTMでは、2つのノードから成るホットスタンバイ冗長化コンセプトが採用されており、冗長性を実現する最低要件となります。Sophos UTMソフトウェ9アに導入された主な改良点の1つに、テイクオーバー(引き継ぎ)のレイテンシを2秒未満に低減できる点があります。ゲートウェイは、ファイアウォール接続の同期化に加え、IPsecトンネルの同期化にも対応してます。つまり、ロードウォリアやリモートVPNゲートウェイが、テイクオーバー後にIPsecトンネルを再度確立する必要はありません。また、隔離されたオブジェクトも同期化されるため、テイクオーバー後も使用可能です。

クラスタ **active-active** :(ベーシックガードサブスクリプションでは使用できません。)大量のインターネットトラフィックのリアルタイム処理に対する需要が高まっています。これに対応するために、Sophos UTMには、処理集約型のタスク(コンテンツフィルタ、ウイルススキャン、侵入防止、復号化など)を複数のクラスタノードに均一に分散するためのクラスタリング機能が用意されています。

専用のハードウェアベースの負荷分散装置を使用する必要なく、ゲートウェイの全体的なパフォーマンスを大幅に向上できます。

注 – クラスタの設定時は、マスタノードを設定してから残りのユニットをスイッチに接続してください。

マスタ、スレーブ、またはワーカの設定手順は非常に似ています。次の手順で実行します。

1. **冗長化オペレーションモードを選択します。**
デフォルトでは、冗長化はオフになっています。次のモードを使用できます。
   - 自動設定
   - ホットスタンバイ（アクティブ–パッシブ）
   - クラスタ（アクティブ–アクティブ）

   注 – 冗長化オペレーションモードを変更する場合、モードを*自動設定*、*ホットスタンバイ*、または*クラスタ*に変更するためには、モードを一度*OFF*に戻す必要があります。

   注 – ライセンス/サブスクリプションが期限切れまたは存在しない場合、オペレーションモード変更が*オフ*および現在のオペレーションモードへと制限されます。

   選択に応じて、1つ以上のオプションが表示されます。

2. **次の設定を行います。**
同期用**NIC**：マスタシステムとスレーブシステムとの通信で経由するネットワークインタフェースカードを選択します。リンクアグリゲーションがアクティブである場合、ここでリンクアグリゲーションインタフェースも選択できます。

   注 – HA同期を、その他ネットワークトラフィックから分離することが推奨されます。例えば、*VLAN*などです。

   注 – まだ設定していないインタフェースのみが表示されます。実行中の設定で同期化インタフェースを変更することができます。その後、すべてのノードはリブートします。

   次のオプションは、オペレーションモードとして*ホットスタンバイ*または*クラスタ*を選択した場合のみ設定できます。

   デバイス名：このデバイスを説明する名前を入力してください。

デバイスノード**ID**: デバイスのノードIDを選択します。プライマリシステムに障害が発生した場合、IDが最も高いノードがマスタとなります。

暗号化キー: マスタとスレーブの通信を暗号化するパスフレーズ(確認のためにパスフレーズを2回入力します)。鍵の最大長は16文字です。

3. *適用***をクリックします。**
   デバイスで冗長化フェイルオーバーがアクティブになりました。

ホットスタンバイモードのゲートウェイは、データ転送接続に対して定期的に更新されます。アクティブなプライマリシステムでエラーが発生した場合、速やかにセカンダリシステムが通常モードに自動的に切り替わり、プライマリシステムの機能を引き継ぎます。

注 – ホットスタンバイシステム/クラスタを無効にすると、スレーブノードとワーカノードは工場出荷時の状態に戻り、シャットダウンします。

詳細情報(特に使用事例)は、SophosKnowledgebaseにある*HA/クラスタガイド*で確認できます。

詳細

このセクションでは、詳細設定を行うことができます。

新しいデバイスの自動設定を有効化: ホットスタンバイシステム/クラスタを手動で設定した場合、このオプションにより、冗長化オペレーションモードが*自動設定*に設定されているデバイスがホットスタンバイシステム/クラスタに自動的に追加されます。ただし、このオプションはスレーブシステムに一切影響を与えないため、デフォルト設定のまま有効にしておくことができます。

Up2Date時にノードをそのまま保持: 選択する場合、新しいシステムバージョンへの更新時に、HA/クラスタノードの半数が現在のシステムバージョンを保持します。新しいバージョンが安定した段階で、*マネジメント* > *冗長化* > *ステータス*ページで残りのノードを更新できます。新しいバージョンのために更新されたすべてのノードで障害が発生する場合は、残りのノードが古いバージョンで新しいHA/クラスタを構築します。その後、障害のあるノードに古いバージョンをインストールするか、新しい更新を待つことができます。

*Up2Date時にノードをそのまま保持*が有効であれば、同期は同じシステムバージョンのノードに限定されるので、予約されたノードは更新後に同期されません。代わりに、予約されたノードの状態が保持されます。そのため、理由によらず予約されたノードの再有効化を決定した場合、更新開始から再有効化までの間の時間に行われたすべての設定変更やレポートデータは失われます。

優先マスタ: ここでは、ドロップダウンリストでノードを選択して、指定のマスタノードを定義できます。フェイルオーバーが発生した場合、選択されたノードはリンクの回復後はスレーブモードのままではなく、マスタモードにスイッチバックします。

バックアップインタフェース: HA同期化インタフェースの障害やネットワークケーブルの切断などが原因で、マスタとスレーブの両方が同時にマスタになること(マスタ/マスタの状況)を防ぐために、バックアップ用のハートビートインタフェースを選択できます。この追加ハートビートインタフェースには、いずれかの設定済みアクティブイーサネットインタフェースを選択できます。バックアップインタフェースを選択すると、マスタ/スレーブ設定が維持されていることを確認するために、このインタフェース経由で追加のハートビート信号が一方向へ(マスタからスレーブへ)送信されます。マスタ/スレーブ接続が無効であり、バックアップインタフェースが関与すると、いずれかのクラスタノードが停止していることを知らせる通知が管理者に送信されます。ただし、このオプションはスレーブシステムに一切影響を与えないため、未設定のままにしておくことができます。

注 – HA同期化インタフェースに障害が発生した場合、設定はそれ以上同期されなくなります。バックアップインタフェースは、マスタ/マスタの状況を回避するだけです。

4.13 シャットダウンとリスタート

このタブでは、手動でSophos UTMをシャットダウンまたはリスタートできます。

シャットダウン: この操作により、システムをシャットダウンして、すべてのサービスを適切に停止できます。モニタやLCDディスプレイが接続されていないシステムの場合は、シャットダウンプロセスの最後にビープ音が1秒間隔で鳴り続けます。

Sophos UTMをシャットダウンするには、以下の手順に従います。

1. *システムをシャットダウン(停止)* をクリックします。
2. **警告メッセージを確認します。**
   【システムをシャットダウンしますか？】というメッセージが表示されたら、*OK*をクリックします。

   システムはシャットダウンして停止します。

お使いのハードウェアおよび設定により、シャットダウンが完了するまでに数分かかる場合があります。システムが完全にシャットダウンした後で、電源を切ります。システムが完全にシャットダウンする前に電源を切ると、システムが次回の起動(ブート)時にファイルシステムの一貫性をチェックするため、起動プロセスに通常よりかなり長く時間がかかることになります。最悪の場合は、データが失われる場合があります。

システムの起動が正常に行われるとビープ音が連続して5回鳴ります。

リスタート: この操作により、システムを完全にシャットダウンして再起動(リブート)します。お使いのハードウェアおよび設定により、完全にリスタートするまでに数分かかる場合があります。

Sophos UTMをリスタートするには、次の手順に従います。

1. *システム をリスタート リブート* をクリックします。

2. **警告メッセージを確認します。**
   【システムをリスタートしますか？】というメッセージが表示されたら、*OK*をクリックします。

   システムはシャットダウンし、停止してからリブートします。

5 定義とユーザ

この章では、Sophos UTM全体で使用されるネットワーク、サービス、期間の定義を設定する方法について説明します。WebAdminの*オブジェクト定義の概要*ページは、タイプに基づくネットワーク定義の数と、プロトコルタイプに基づくサービス定義の数を示します。

*定義とユーザ*メニューのページを使用すると、他のすべての設定メニューで使用することが可能なネットワークとサービスを一元的に定義することができます。これにより、IPアドレス、ポート、ネットワークマスクなどに悩まされることなく、名前を使用して作業できます。その他のメリットとしては、個々のネットワークやサービスをグループにまとめて、一度に設定できることがあげられます。後でこれらのグループに特定の設定を割り当てたりすると、これらの設定はグループに含まれるすべてのネットワークとサービスに適用されます。

さらに、Sophos UTMこの章では、のユーザアカウント、ユーザグループ、および外部認証サーバの設定方法や、クライアントPCの認証について説明します。

この章には次のトピックが含まれます。

- ネットワーク定義
- サービス定義
- 時間帯定義
- ユーザとグループ
- クライアント認証
- 認証サービス

5.1 ネットワーク定義

定義とユーザ > *ネットワーク定義*メニューを使用して、ホスト、ネットワーク、ネットワークグループ、ならびにMAC アドレス定義を作成することができます。ここで作成した定義は、他の多くのWebAdmin設定でも使用できます。

5.1.1 ネットワーク定義

定義とユーザ > *ネットワーク定義* > *ネットワーク定義*タブは、UTMのホスト、ネットワーク、ネットワークグループを一元的に定義する場所です。ここで作成した定義は、他の多くのWebAdmin設定メニューでも使用できます。

デフォルトでは、タブを開くとすべてのネットワーク定義が表示されます。リストの上部のドロップダウンリストを使用して、特定のプロパティを持つネットワーク定義を表示するように選択できます。

ヒント – *ネットワーク定義*リストでネットワーク定義の情報アイコンをクリックすると、ネットワーク定義が使用されているすべての設定項目を表示できます。

ネットワークテーブルには、システムが自動的に作成した、編集も削除もできないスタティックネットワークも含まれています。

- 内部 *アドレス*：このタイプの定義は、各ネットワークインタフェースに追加されます。ここには、インタフェースの現在のIPアドレスが含まれています。名前では、インタフェース名の後に「(Address)」という言葉が付いています。
- 内部 *ブロードキャスト*：このタイプの定義は、各イーサネットタイプネットワークインタフェースに追加されます。ここには、インタフェースの現在のIPv4ブロードキャストアドレスが含まれています。名前では、インタフェース名の後に「(Broadcast)」という言葉が付いています。
- 内部 *ネットワーク*：このタイプの定義は、各イーサネットタイプネットワークインタフェースに追加されます。ここには、インタフェースの現在のIPv4ネットワークが含まれています。名前では、インタフェース名の後に「(Network)」という言葉が付いています。
- あらゆる **IPv4/IPv6**：インタフェースに関連付けられたネットワーク定義(それぞれIPv4、およびIPv6が有効な場合はIPv6用)。設定でこれを使用すると、設定プロセスが容易になります。アップリンクバランスを有効にすると、*インターネット*定義は*アップリンクインタフェース*と関連付けられます。

  注 – IPv6エントリは、*インタフェース& ルーティング* > *IPv6*で有効になっている場合にのみ表示されます。

注 – クライアント認証によって認証されたユーザネットワークのオブジェクトは、パフォーマンス上の理由から、必ず未解決として表示されます。

ネットワーク定義を作成するには、次の手順に従います。

1. ***ネットワーク定義*タブで、*新規ネットワーク定義*をクリックします。**
   *ネットワーク定義の追加*ダイアログボックスが開きます。
2. **次の設定を行います。**

(選択した定義タイプに応じて、ネットワーク定義のさらに詳細なパラメータが表示されます。)

名前：この定義を説明する名前を入力してください。

タイプ: ネットワーク定義タイプを選択します。次のタイプを使用できます。

- ホスト: 単一IPアドレス。次の情報を指定します。
  - **IPv4**アドレス/**IPv6**アドレス: ホストのIPアドレス(設定されたインタフェースのIPアドレスを入力することはできません)。
  - **DHCP**設定(オプション):このセクションで、ホストとIPアドレス間のスタティック(静的)マッピングを作成できます。これには、設定されたDHCPサーバーが必要になります(*ネットワークサービス > DHCP > サーバー*参照)。

注 – DHCPプールから通常通りに割り当てられたアドレスとスタティックにマッピングされたアドレスの間でIPアドレスの重複が発生することを防止するために、スタティックにマッピングする場合はDHCPプールの範囲外のアドレスを指定してください。たとえば、DHCP プールが `192.168.0.100`～`192.168.0.210` である場合にスタティックマッピングとして `192.168.0.200` を指定すると、2つのシステムが同じIP アドレスを持つことになります。

IPv4 DHCP: スタティックマッピングに使用するIPv4 DHCPサーバを選択します。

MACアドレス: ホストのネットワークインタフェースカードのMACMACアドレスは通常、2桁の16進数をコロンまたはハイフンで区切って6組まとめた形式で指定します(`00:04:76:16:EA:62`など)。アドレスを入力します。

IPv6 DHCP: スタティックマッピングに使用するIPv6 DHCPサーバを選択します。

DHCPの一意の**ID**: ホストのDUIDを入力します。Windowsなどのオペレーティングシステムの場合、DUIDはWindowsレジストリで確認できます。`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\TCPIP6\Parameters`

2桁の16進数をコロンで区切ってまとめた形式で指定します（00:01:00:01:13:30:65:56:00:50:56:b2:07:51など）。

- **DNS**設定（オプション）：独自のDNSサーバの設定は必要としないが、ネットワークの一部のホストでDNSスタティックマッピングが必要な場合は、それぞれのホストのこのセクションにこれらのマッピングを入力することができます。これは限られた数のホストにしか対応できないため、フルオペレーションを行っているDNSサーバの代わりに使用することは決してしないでください。

  ホスト名：ホストの完全修飾ドメイン名（FQDN）を入力します。

  リバース**DNS**：ホストのIPアドレスと名前のマッピングを有効化するには、チェックボックスにチェックを入れます。同じIPアドレスに複数の名前をマッピングすることが可能ですが、1つのIPアドレスには1つの名前にしかマッピングできません。

  追加ホスト名：「+」アイコンをクリックして、ホストに追加ホスト名を追加します。

- **DNS**ホスト：DNSホスト名。システムによってダイナミックに解決され、IPアドレスが生成されます。DNSホストは、ダイナミックIPエンドポイントの使用時に便利です。システムは、TTL（生存時間）の値に従って定期的にこれらの定義を再解決し、新しいIPアドレスがある場合は定義を更新します。次の情報を指定します。

  - ホスト名：リゾルブしたいホスト名。

- **DNS**グループ：**DN**Sホストと似ていますが、1つのホスト名用のDNS内の複数のRR（リソースレコード）を処理できます。透過プロキシでのファイアウォールルールと除外の定義に便利です。

- ネットワーク：標準的なIPネットワーク。ネットワークアドレスとネットマスクから構成されています。次の情報を指定します。

  - **IPv4**アドレス/**IPv6**アドレス：ネットワークのネットワークアドレス（設定されたインタフェースのIPアドレスを入力することはできません）。

  - ネットマスク：オクテット内のいくつのビットでサブネットワークが指定され、いくつのビットがホストアドレスに使用されるかを示すために使用されるビットマスク。

- レンジ：IPv4アドレスレンジの全範囲を定義するために選択します。次の情報を指定します。

- **IPv4**開始アドレス: 範囲で最初のIPv4アドレスです。
- **IPv4**終了アドレス: 範囲で最後のIPv4アドレスです。
- **IPv6**開始アドレス: 範囲で最初のIPv6アドレスです。
- **IPv6**終了アドレス: 範囲で最後のIPv6アドレスです。

- マルチキャストグループ: 定義されたマルチキャストネットワーク範囲から構成されるネットワーク。
  - **IPv4**アドレス: マルチキャストネットワークのネットワークアドレス。`224.0.0.0`～`239.255.255.255`の範囲である必要があります。
  - ネットマスク: オクテット内のいくつのビットでサブネットワークが指定され、いくつのビットがホストアドレスに使用されるかを示すために使用されるビットマスク。
- ネットワークグループ: 他のネットワーク定義のリストが含まれるコンテナ。これらを使用してネットワークとホストをまとめると、設定がより読みやすくなります。*ネットワークグループ*を選択すると、*メンバー*ボックスが表示され、グループメンバーを追加できます。
- 可用性グループ: ホストまたは**DNS**ホスト(あるいはその両方)のグループ。すべてのホストの生存ステータスがICMP pingにより、デフォルトで60秒間隔でチェックされます。優先順位が最も高く、生存ステータスであるホストが設定で使用されます。*アベイラビリティグループ*を選択すると、*メンバー*ボックスが表示され、グループメンバーを追加できます。

コメント(オプション):説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**
表示されるオプションは、上で選択されている*タイプ*に依存します。

インタフェース(オプション):ネットワーク定義を特定インタフェースにバインドして、その定義への接続がこのインタフェース経由でのみ確立されるようにすることができます。

モニタリングタイプ: (*アベイラビリティグループ*タイプのみ):生存ステータスチェックのサービスプロトコルを選択します。モニタリング用に*TCP*(TCP 接続の確立)、*UDP*(UDP 接続の確立)、*Ping*(ICMP Ping)、*HTTP ホスト*(HTTP 要求)、または*HTTPS ホスト*(HTTPS 要求)のいずれかを選択します。*UDP*を使用する場合、ping要求が最初に送信され、成功した場合は、続いてペイロード0のUDP パケットが送信されます。pingが成功しなかった場合や、ICMPポートに到達できない場合、このホストはダウンしているとみなされます。

ポート(*TCP*または*UDP*のモニタリングタイプのみ):要求の送信先のポート番号。

URL(オプション、*HTTPホスト*または*HTTPSホスト*のモニタリングタイプのみ):要求するURL。URLにポート情報を追加することで、デフォルトポートの80または443以外のポートを使用することもできます。例、`http://example.domain:8080/index.html`。URLを指定しない場合は、ルートディレクトリが要求されます。

間隔:ホストをチェックする間隔を秒単位で入力します。

タイムアウト:が応答を送信する最大時間を秒単位で入力します。ホストがこの時間内に応答しない場合、デッド(dead)とみなされます。

常にリゾルブ:このオプションはデフォルトで選択されているため、すべてのホストが使用不可である場合、グループは最後に使用可能であったホストで解決されます。チェックを外すと、すべてのホストがデッド(dead)の場合は、グループが*未解決*に設定されます。

4. ***保存*をクリックします。**
   新しい定義がネットワーク定義リストに表示されます。

ネットワーク定義を編集または削除するには、対応するボタンをクリックします。

5.1.2 MACアドレス定義

*定義とユーザー > ネットワーク定義 > MACアドレス定義*タブは、MACアドレスリストなどのMACアドレスの定義を一元的に設定する場所です。MACアドレス定義は、ネットワーク定義と同様に使用できます。MACアドレスの定義によって、ホストやIPアドレスに基づいたルールをさらに定義済みのMACアドレスを持つデバイスにマッチするものだけに限定するために使用できます。

ヒント – 「MACアドレス定義」の情報アイコンをクリックすると、この定義が使用されているすべての設定オプションを表示できます。

MACアドレス定義を作成するには、次の手順に従います。

1. ***MACアドレス定義*タブで、*新規MACアドレスリスト*をクリックします。**
   *MACアドレスリストの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:この定義を説明する名前を入力してください。

MAC *アドレス*:「+」アイコンをクリックして個々のMACアドレスを入力するか、アクションアイコンを使用してコピー&ペーストでMACアドレスのリストをインポートします。MACアドレスは通常、2桁の16進数をコロンまたはハイフンで区切って6組まとめた形式で指定します(`00:04:76:16:EA:62`など)。

ホスト: MACアドレス定義に追加したいMACアドレスを持つホストを追加または選択します。ホスト定義の*DHCP設定*セクションで定義されたMACアドレスが、MACアドレスリストに追加されます。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

注 – アドレス定義当たりのアドレスの数は、以下の使用例に制限されます:ワイヤレスネットワークへのアクセスを制限するには、最大で200です。REDアプライアンスへのアクセスを制限するには、RED 10で最大200、RED 50で最大400です。

注 – MACアドレスまたはホストのどちらか一方または両方入力することができます。

コメント(オプション):説明などの情報を追加します。

3. ***保存*をクリックします。**
   新しい定義が*MAC アドレス定義*リストに表示されます。

MACアドレス定義を編集あるいは削除するには、該当するボタンをクリックします。

5.2 サービス定義

定義とユーザ > *サービス定義*ページで、サービスおよびサービスグループを定義して一元管理できます。サービスは、特定タイプのネットワークトラフィックの定義で、TCP や UDP といったプロトコルに関する情報とプロトコル関連オプション(ポート番号など)に関する情報を組み合わせています。サービスを使用して、UTMで許可または拒否されるトラフィックのタイプを決定することができます。

ヒント – *サービス定義*リストのサービス定義の情報アイコンをクリックすると、サービス定義が使用されているすべての設定オプションを表示できます。

サービス定義を作成するには、以下の手順に従います。

1. ***サービス定義*ページで*新規サービス定義*をクリックします。**
   *サービス定義の追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
(選択した定義タイプに応じて、サービス定義のさらに詳細なパラメータが表示されます。)

名前 : この定義を説明する名前を入力してください。

定義タイプ: サービスタイプを選択します。次のタイプを使用できます。

- **TCP**: TCP (Transmission Control Protocol) 接続では、0〜65535のポート番号を使用します。ロストしたパケットはTCPが認識して再度リクエストします。TCP接続では、受信者は送信者に対してデータパケットを受信したときに通知します(接続関連のプロトコル)。TCPセッションは3WAYハンドシェークで始まり、セッションの最後に接続がクローズします。次の情報を指定します。
  - 宛先ポート: 宛先ポートを単一のポート番号(例:80)あるいは範囲(例:1024:64000)として入力します。範囲を指定する場合は、コロンを区切り文字として使用します。
  - 送信元ポート: 送信元ポートを単一のポート番号(例:80)あるいは範囲(例:1024:64000)として入力します。範囲を指定する場合は、コロンを区切り文字として使用します。
- **UDP**: *UDP User Datagram Protocol* は、0〜65535のポート番号を使用するステートレスプロトコルです。UDPはステートを維持しないため、TCPより高速です。特に、少量のデータは高速に送信できます。ただし、このステートレスであるということは、UDPはパケットがロストまたはドロップした場合に認識できないことも意味します。受信コンピュータは、データパケットを受信しても送信者に通知しません。*UDP*を選択した場合は、TCPの場合と同じ設定オプションを編集できます。
- **TCP/UDP**: TCPとUDPの組み合わせで、DNSなどの両方のサブプロトコルを使用するアプリケーションプロトコルに適切です。*TCP/UDP*を選択した場合は、TCPまたはUDPの場合と同じ設定オプションを編集できます。
- **ICMP/ICMPv6**: *ICMP Internet Control Message Protocol* は主にエラーメッセージの送信に使用されます。たとえば、要求されたサービスが利用できない、あるいはホストやルータに到達できなかった、などのメッセージを送信します。*ICMP* または *ICMPv6* を選択した場合は、ICMP コード/タイプを選択します。IPv4ファイアウォールルールはICMPv6では機能せず、IPv6ファイアウォールルールはICMPでは機能しません。
- **IP**: *IP Internet Protocol* は、インターネット上でのデータのやり取りに使用されるネットワークおよび伝送プロトコルです。*IP* を選択したら、IP内でカプセル化されるプロトコルの番号を指定します(例:121、これは SMP プロトコルを表します)。

- **ESP**:*ESP*(カプセル化セキュリティペイロード)は、IPsecトンネリングプロトコルスイートの一部で、VPNを介してトンネルされるデータに暗号化サービスを提供します。ESPまたはAHを選択した場合は、*セキュリティパラメータインデックス*(SPI)を指定します。これは、IPアドレスとともにセキュリティパラメータを特定します。特に自動IPsec鍵交換を使用する場合は、256～4,294,967,296の値を入力するか、または256～4,294,967,296の範囲として指定されたデフォルト設定を使用します(コロンを区切り文字として使用します)。1～255の番号は*IANA*(Internet Assigned Numbers Authority)によって予約されています。
- **AH**:*認証ヘッダー AH* はIPsecトンネリングプロトコルスイートの一部で、IPヘッダとデータグラムペイロード間に位置し、情報の(機密性ではなく)整合性を維持します。
- *グループ*:他のサービス定義リストを含むコンテナ。設定を読みやすくするために、これらを使用してサービス定義をまとめることができます。*グループ*を選択すると、*メンバー*ボックスが開くので、そこでグループのメンバー(その他のサービス定義など)を追加します。

コメント(オプション):説明などの情報を追加します。

3. ***保存*をクリックします。**
   新しい定義が*サービス定義*リストに表示されます。

定義を編集または削除するには、対応するボタンをクリックします。

注 – 定義タイプは後で変更できません。定義タイプを変更するには、サービス定義を削除し、希望の設定で新しいサービス定義を作成します。

5.3 時間帯定義

定義およびユーザ > *期間定義*ページで、単独または繰り返し発生する時間帯(タイムスロット)を定義できます。これを使用して、コンテンツフィルタプロファイルの割り当てを特定の時間範囲に制限できます。

ヒント - *時間帯定義*リストの時間帯定義の情報アイコンをクリックすると、その時間帯定義が使用されているすべての設定オプションを表示できます。

時間帯定義を作成するには、次の手順に従います。

1. ***時間帯定義*タブで、*新規時間帯定義*をクリックします。**
   *時間帯定義の追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前：この時間帯定義を説明する名前を入力します。

   タイプ：時間帯定義のタイプを選択します。次のタイプを使用できます。

   - 繰り返しイベント：これらのイベントは定期的に繰り返されます。開始時間、終了時間、および時間帯定義が適用される曜日を選択できます。終了時間が翌日になる場合は、開始時間の曜日を選択します。このタイプには開始日と終了日は選択できません。
   - 単独イベント：これらのイベントは一度だけ実施されます。開始日時および終了日時の両方を選択できます。これらの定義は繰り返されないので、*曜日*オプションはこのタイプには選択できません。

   コメント（オプション）：説明などの情報を追加します。

3. ***保存*をクリックします。**
   新しい時間帯定義が*時間帯定義*リストに表示されます。

時間帯定義を編集あるいは削除するには、該当するボタンをクリックします。

5.4 ユーザとグループ

定義とユーザ > *ユーザとグループ*メニューを使用して、WebAdminアクセス、およびリモートアクセス、ユーザポータルアクセス、メールの使用などのための、ユーザとグループを作成できます。

5.4.1 ユーザ

定義とユーザ > *ユーザとグループ* > *ユーザ*タブで、UTMにユーザアカウントを追加することができます。Sophos UTMには、工場出荷時のデフォルト設定として、*admin*という1人の管理者が構成されています。

> ヒント – *ユーザ*リストのユーザ定義の情報アイコンをクリックすると、ユーザ定義が使用されているすべての設定オプションを表示できます。

*新規ユーザ*ダイアログボックスでメールアドレスを指定すると、このユーザのX.509証明書が生成されるのと同時に、メールアドレスを証明書のVPNIDとして使用してユーザ定義が作成されます。メールアドレスが指定されていない場合は、ユーザの*識別名*（DN）をVPN IDとして証明書が作成されます。このように、ユーザがeDirectoryなどのバックエンドグループにより認証されている場合

は、対応するバックエンドユーザオブジェクトでメールアドレスが設定されていない場合でも証明書は作成されます。

なぜなら、各証明書のVPN IDは一意であるため、各ユーザ定義は異なる一意のメールアドレスを使用しているからです。システムにすでにあるEメールアドレスを使用したユーザ定義の作成は失敗します。証明書は、Sophos UTMがサポートする各種リモートアクセス方法で使用可能です。ただし、PPTP、PSKを使用するL2TP over IPsec、およびRSAまたはPSKを使用するネイティブIPsecは除外されます。

ユーザアカウントを追加するには、以下の手順に従います。

1. ***ユーザー*タブで、*新規ユーザー*をクリックします。**
   *ユーザの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   ユーザ名：このユーザを説明する名前を入力します（例：jdoe）。PPTPまたはL2TP over IPsec経由のリモートアクセスを使用する場合、パスワードには印刷可能なASCII文字しか使用できないことがあります[1]。

   実際の名前：ユーザの実際の名前を入力します（例：John Doe）。

   メールアドレス：ユーザのプライマリメールアドレスを入力します。

   他の*メールアドレス*（オプション）：このユーザの他のメールアドレスを入力します。これらのEメールアドレスに送信されたスパムメールは各Eメールアドレス用の個々の隔離レポートにリストされ、このレポートは前述のプライマリEメールアドレスに送信されます。

   認証：認証方式を選択します。以下の方式を使用できます。

   - *ローカル*：この方式は、UTMでユーザをローカル認証する場合に選択します。
   - リモート：Sophos UTMでサポートされている外部認証方式のいずれかを使用してユーザを認証する場合に選択します。詳細は、*定義とユーザ* > *認証サービス*を参照してください。
   - なし：ユーザが認証されるのを完全に防止する場合に選択します。これは、たとえば、ユーザ定義を削除することなくユーザを一時的に無効にする場合に役に立ちます。

   パスワード：ユーザのパスワードを入力します（確認のために2回入力します）。認証方式として*ローカル*を選択した場合のみ利用できます。基本的なユーザ認証ではウムラウトはサ

[1] http://en.wikipedia.org/wiki/ASCII#ASCII_printable_characters

ポートしていません。PPTPまたはL2TP over IPsec経由でリモートアクセスを使用する場合、ユーザ名には、ASCII印字可能文字[1]だけが含まれています。

バンクエンドの同期：実際の名前やユーザのメールアドレスなどのユーザ定義の基本設定の一部を、データを外部バックエンド認証サーバと同期することで自動的に更新できます（認証方式として *リモート*を選択したときのみ利用できます）。ユーザがプリフェッチで選択されていると、オプションは*認証サービス* > *詳細*タブの *ログイン時のバックエンド同期を有効化*オプションで自動的に設定されます。

注 - 現在は、Active DirectoryおよびeDirectoryサーバーのデータのみ同期できます。

X.509証明書：ユーザ定義を作成したら、ユーザ定義を編集する際にこのユーザにX.509証明書を割り当てることができます。デフォルトでは、この証明書はユーザ定義を作成したときに自動的に生成されたものです。ただし、サードパーティの証明書を割り当てることもできます。証明書は、*リモートアクセス* > *証明書管理* > *証明書*タブでアップロードできます。

スタティックリモートアクセス**IP**を使用 オプション ：リモートアクセスを取得するユーザに、IPアドレスプールのダイナミックIPアドレスを割り当てる代わりにスタティックIPアドレスを割り当てる場合に選択します。NATルータ背後のIPsecユーザは、スタティックリモートアクセスIPアドレスを必ず使用する必要があります。

注 - スタティックリモートアクセスIPは、PPTP、L2TP、およびIPsecを介したリモートアクセスのみに使用できます。これは、SSLを介したリモートアクセスには使用できません。

コメント(オプション)：説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**
   ユーザは独自のメールホワイトリストとブラックリストを作成し、管理することができます（ユーザポータルの章を参照）。ここでこれらのリストを参照し、必要に応じて変更することができます。

4. *保存***をクリックします。**
   新しいユーザアカウントが *ユーザ*リストに表示されます。

このユーザをWebベースの管理インタフェースWebAdminへのアクセスをもつ正規の管理者にする場合は、そのユーザを*SuperAdmins*グループに追加します。SuperAdminsは、WebAdminの *定義とユーザ* > *ユーザとグループ* > *グループ*タブで設定します。

[1] http://en.wikipedia.org/wiki/ASCII#ASCII_printable_characters

注 – ユーザーオブジェクトを削除した後で同じ名前でユーザーオブジェクトを作成する場合は、このユーザーに関連する証明書も*リモートアクセス* > *証明書管理* > *証明書*タブで削除したことを確認してください。削除していない場合、「その名前のアイテムはすでに存在します」という旨のエラーメッセージが表示されます。

何らかのリモートアクセスが有効化されたユーザのリモートアクセス証明書や設定をダウンロードすることができます。このためには、各ユーザの前にあるチェックボックスにチェックを入れ、リストヘッダの*アクション*ドロップダウンリストから目的のオプションを選択します。ユーザポータルの使用が許可されている場合は、リモートアクセスユーザ自身もこれらのファイルをダウンロードできます。

5.4.2 グループ

定義とユーザ > *ユーザとグループ* > *グループ*ページで、UTMにユーザグループを追加することができます。Sophos UTMには、工場出荷時のデフォルト設定として、*SuperAdmins*というユーザグループがあります。管理特権をユーザに割り当てたい(つまりWebAdminへのアクセス権をユーザに付与したい)場合は、当該ユーザを*SuperAdmins*グループに追加します。このグループは削除しないでください。

ヒント – *グループ*リストでグループの定義をクリックすると、そのグループ定義が使用されているすべての設定オプションが表示されます。

ユーザグループを追加するには、次の手順に従ってください。

1. ***グループ*タブで、*新規グループ*をクリックします。**
   *グループの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   グループ名：このグループを説明する名前を入力してください。この名前は、バックエンドグループの名前に対応している必要はありません。

   グループタイプ: グループのタイプを選択します。静的メンバのグループか、動的メンバシップを実現する2種類のグループタイプから選択できます。

   - *スタティックメンバ*: このグループのメンバとなるローカルユーザを選択します。

- **IPsec X509 DN**マスク: ユーザは、IPsec接続によってゲートウェイへのログインに成功し、識別名に含まれる特定のパラメータがDNマスクボックスで指定された値と一致した場合に、*IPsec* X509 DNグループ定義に動的に追加されます。
- バックエンドメンバシップ: ユーザは、サポートされるいずれかの認証メカニズムによる認証が成功した場合に、グループ定義に動的に追加されます。続行するには、該当するバックエンド認証タイプを選択します。
  - **Active Directory**: UTMのActive Directoryユーザグループは、Windowsネットワーク上で設定されているActive Directoryサーバユーザグループのメンバに対し、グループメンバシップを提供します。詳細は、*定義とユーザ* > *認証サービス* > *サーバ*を参照してください。
  - **eDirectory**: UTMのeDirectoryユーザグループは、eDirectoryネットワーク上で設定されているeDirectoryユーザグループのメンバに対し、グループメンバシップを提供します。詳細は、*定義とユーザ* > *認証サービス* > *サーバ*を参照してください。
  - **RADIUS**: ユーザは、RADIUS認証方式による認証が成功すると、RADIUSバックエンドグループに自動的に追加されます。
  - **TACACS+**: ユーザは、TACACS+認証方式による認証が成功すると、TACACS+バックエンドグループに自動的に追加されます。
  - **LDAP**: ユーザは、LDAP認証方式による認証が成功すると、LDAPバックエンドグループに自動的に追加されます。

バックエンドグループメンバシップに制限（オプション、バックエンドグループ*Active Directory*または*eDirectory*だけ）: 選択したバックエンドサーバのすべてのユーザをこのグループ定義に含めることを望まない場合は、すべてのX.500ベースのディレクトリサービスに対して、バックエンドサーバ上のいくつかのグループにメンバシップを制限することができます。このオプションを選択する場合、ここで入力するグループは、バックエンドサーバに設定されている*一般名*と一致している必要があります。Active Directoryバックエンドに対してこのオプションを選択する場合、`CN=`プレフィックスは省略できます。eDirectoryバックエンドに対してこのオプションを選択すると、eDirectoryブラウザを使用して、このグループ定義に含めるeDirectoryグループを簡単に選択することができます。ただし、eDirectoryブラウザを使用しない場合は、eDirectoryコンテナの入力時に`CN=`プレフィックスを必ず含めてください。

LDAP属性のチェック（オプション、バックエンドグループ*LDAP*の場合だけ）: 選択したバックエンドLDAPサーバのすべてのユーザをこのグループ定義に含めたくはない場合は、このチェックボックスにチェックを入れて、バックエンドサーバ上にある特定

のLDAP属性に一致するユーザのみにメンバシップを制限することができます。この属性はLDAP検索フィルタとして使用されます。たとえば、属性として`groupMembership`を入力し、その値として`CN=Sales,O=Example`を入力することにより、そうすると、会社の営業部門に属するすべてのユーザをグループ定義に含めることができます。

コメント(オプション):説明などの情報を追加します。

3. ***保存*をクリックします。**
   新しいユーザグループが*グループ*リストに表示されます。

グループを編集または削除するには、対応するボタンをクリックします。

5.5 クライアント認証

Sophosは、UTMで直接ユーザ認証を行うために、WindowsおよびMac OS用の認証クライアントを提供しています。これにより、ユーザネットワークまたはグループネットワークに基づくファイアウォールルールを作成したりすることで、Webサーフィンやネットワークトラフィックをユーザに基づいてコントロールすることができます。さらに、可能であれば、IPアドレス、ホスト名、その他の情報をユーザ名に置き換えるため、データやオブジェクトのレポートがより読みやすくなります。

注 – WebAdminでは、クライアント認証によって認証されたユーザネットワークのオブジェクトは、パフォーマンス上の理由から、必ず未解決として表示されます。

クライアント認証を使用したい(あるいは使用する必要がある)ユーザは、クライアントPCまたはMac OSコンピュータにSophos Authentication Agent(SAA)をインストールする必要があります。SAAは、このWebAdminページまたはユーザポータルからダウンロード可能です。ユーザポータルのページにダウンロードリンクが表示されるのは、クライアント認証設定のユーザグループに参加しているユーザのみです。

クライアント認証を設定するには、次の手順に従ってください。

1. ***クライアント認証*タブで、クライアント認証を有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチが緑色になり、*クライアント認証 オプション*エリアが編集可能になります。

2. **許可するネットワークを選択します。**
   クライアント認証を使用する必要があるネットワークを追加または選択します。クライアント認証が機能するためには、これらのネットワークがUTMに直接接続されている必要があり

ます。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

3. **許可するユーザおよびグループを選択します。**
単一のユーザおよびグループを*許可されるユーザおよびグループ*ボックスで選択、または新規ユーザを追加します。これは、既存の認証グループ(Active Directoryユーザグループなど)にすることもできます。ユーザを追加する方法は、*定義とユーザ* > *ユーザとグループ* > *ユーザ*ページで説明しています。

4. ***適用*をクリックします。**
設定が保存されます。

選択したネットワークでクライアント認証を利用できるようになりました。

クライアント認証プログラム

クライアント認証を有効にすると、ここでSophos Authentication Agent (SAA)をダウンロードできます。SAAを手動で配布するか、ユーザがユーザポータルからダウンロードできるようにすることができます。

EXEのダウンロード: クライアントPCに直接インストールするためのCA証明書を含むクライアント認証プログラムをダウンロードします。これは、ユーザポータルからダウンロードできるファイルと同じです。

MSIのダウンロード: クライアント認証MSI パッケージをダウンロードします。このパッケージは、ドメインコントローラ(DC)による自動パッケージインストール用に設計されていて、CA証明書は含んでいません。

DMGのダウンロード: クライアント認証Mac OS Xディスクイメージをダウンロードします。このイメージは、OS Xオペレーティングシステムが搭載されているクライアントコンピュータにインストールするように設計されています。

CAのダウンロード: MSI パッケージに加えて展開する必要があるCA証明書をダウンロードします。

SAAはWebフィルタの認証モードとして使用できます。詳しくは、*Webプロテクション*」>「*Webフィルタリング*」>「*グローバル*の章を参照してください。

5.6 認証サービス

定義とユーザ > *認証サービス*ページでは、シングルサインオンまたはワンタイムパスワードなどの外部ユーザ認証サービスのデータベースおよびバックエンドサーバを管理できます。外部ユーザー認証を使用すると、ネットワーク内の他のサーバー上にある既存のユーザーデータベースや

ディレクトリサービスに対して、ユーザーアカウントを検証することができます。現在サポートされている認証サービスは次のとおりです。

- NovellのeDirectory
- マイクロソフトのActive Directory
- RADIUS
- TACACS+
- LDAP

5.6.1 グローバル設定

定義とユーザ > *認証サービス* > *グローバル設定*タブを使用すると、基本的な認証オプションを設定できます。次のオプションを使用できます。

自動的にユーザを作成: このオプションを選択した場合、設定済みのバックエンドグループの不明ユーザが、Sophos UTMでサポートされている各種認証サービスのいずれかに対する認証に成功すると、Sophos UTMは常にユーザオブジェクトを自動作成します。例えば、RADIUSバックエンドグループを設定しており、*マネジメント* > *WebAdmin設定* > *アクセスコントロール*タブで定義したいずれかのロールにこのグループをメンバーとして追加する場合、Sophos UTM は WebAdmin へのログインに成功したRADIUSユーザーに対してユーザー定義を自動的に作成します。

- **機能別自動ユーザ作成:** 自動ユーザ作成は、特定のサービスに対して有効または無効にすることができます。有効なサービスに対してのみ、ユーザが作成されます。*自動的にユーザを作成*オプションからチェックを外すと、このオプションは使用できず、ユーザの自動作成機能はすべての機能に対して無効になります。

  > **注 –** この機能は、Active Directory*のシングルサインオン*(SSO)では機能しません。

これらのユーザーオブジェクトは、Sophos UTMのユーザーポータルへのアクセス権を付与するためにも必要になります。さらに、自動作成されたすべてのユーザーオブジェクトのために、X.509証明書が生成されます。ただし、Eメールアドレスが衝突する場合は、このユーザの自動作成は失敗します。この理由は、自動的に作成されるユーザ定義において、システムにすでに存在するEメールアドレスを設定すべきではないためです。すべてのEメールアドレスは、X.509証明書の識別子として使用されるため、システム内で一意でなければなりません。

> **重要 –** ユーザーオブジェクトが自動作成されたユーザーに対する認証(ユーザーが何者であるかを判断するためのアクション)と権限付与(ユーザーが何を許可されているかを判断するため

のアクション)は、常にリモートのバックエンドサーバー/ディレクトリサービス上で実行されます。そのため、対応するバックエンドサーバが使用不能な場合や、そのリモートサイトでユーザオブジェクトが削Sophos UTM除されている場合には、で自動的に作成されたユーザオブジェクトは機能しません。

また、Active Directoryの*シングルサインオン*(SSO)を除き、Sophos UTMはリモート認証サーバから取得したユーザ認証データを300秒間キャッシュします。このため、リモートユーザ設定への変更は、キャッシュの期限が切れた後で初めて有効になります。

認証キャッシュ

Sophos UTMが不明ユーザから`http`などのユーザ要求を受信し、認証が必要である場合は、Sophosが必ず認証キャッシュにエントリを書き込みます。長期的に、ユーザが頻繁に変わるような環境では、適宜キャッシュを空にすることが合理的です。また、すべてのユーザに対して、新たな認証を今すぐ強制したい場合には、また、すべてのユーザに対して、新たな認証を今すぐ強制したい場合には、*認証キャッシュをクリア*ボタンを使用して、認証キャッシュを空にしてください。
認証は300秒間有効です。この間、同じユーザから他の認証要求があったときには、直接キャッシュが検索されます。この方法により、eDirectoryなどのバックエンド認証サービスにかかる負荷を軽減できます。

注 – キャッシュのクリアは、リモートログイン中のユーザには影響がありません。

ライブログ

ライブログを開く: このボタンをクリックすると、新しいウィンドウに *SophosUser Authentication* (SUA)のログが表示されます。

5.6.2 サーバ

定義とユーザ > *認証サービス* > *サーバ*タブで、1つ以上の認証サーバを作成できます。作成するには以下のリンクに従ってください。

- eDirectory
- Active Directory
- LDAP
- RADIUS
- TACACS+

5.6.2.1 eDirectory

Novell eDirectoryは、あるネットワーク内の複数のサーバとコンピュータ上にあるリソースへのアクセスを一元管理するためのX.500互換ディレクトリサービスです。eDirectoryは階層構造のオブジェクト指向データベースであり、組織内のすべての資産を論理ツリーで表現します。資産には、人、サーバ、ワークステーション、アプリケーション、プリンタ、サービス、グループなどが含まれます。

eDirectory認証を設定するには、次の手順に従ってください。

1. ***サーバ*タブで、*新規認証サーバ*をクリックします。**
   *認証サーバの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   バックエンド: バックエンドのディレクトリサービスとして*eDirectory*を選択します。

   位置: バックエンドサーバの位置を選択します。番号が小さいバックエンドサーバから順に問い合わせが行われます。パフォーマンスを向上するためには、要求を最も多く受けると予想されるバックエンドサーバをリストの一番上に配置します。

   サーバ: eDirectoryサーバを選択または追加します。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

   SSL: SSLデータ転送を有効にするには、このオプションを選択します。すると、*ポート*が389(LDAP)から636(ldaps = LDAP over SSL)に変わります。

   ポート: eDirectoryサーバのポートを入力します。デフォルトで、ポート389が選択されています。

   バインド**DN**: サーバにバインドするユーザの*識別名*(DN)を指定します。eDirectory サーバーへの匿名での問い合わせが許可されていない場合、このユーザーが必要です。このユーザには、関連するすべてのユーザオブジェクト情報をeDirectoryサーバから取得してユーザの認証を行うために必要な特権が付与されている必要があります。eDirectoryユーザ、グループ、コンテナは、LDAP表記法で完全識別名として指定します。区切り文字にはコンマを使用します(例:`CN=administrator,DC=intranet,DC=example,DC=com`)。

   パスワード: バインドユーザのパスワードを入力します。

   サーバ設定のテスト: *テスト*ボタンを押すと、設定されたサーバとのバインドテストが実行されます。これにより、このタブの設定が正しいこと、およびサーバーが起動しており、接続を受け付けていることが確認されます。

ベースDN：LDAPツリーのルートに相対的な開始位置で、ここに認証されるユーザが含まれています。ベース DN は、LDAP 表記の完全識別名 (FDN) で、コンマを区切り文字として使用して指定する必要があります (例: `O=Example,OU=RnD`)。ベースDNは空にすることもできます。この場合は、ベースDNは自動的にディレクトリから取り出されます。

ユーザ名：認証を実行するテストユーザのユーザ名を入力してください。

パスワード：テストユーザのパスワードを入力します。

サンプルユーザの認証：*テスト*ボタンをクリックして、テストユーザの認証テストを開始します。これにより、すべてのサーバ設定が正しいこと、サーバが稼働中で接続を受け付けていること、およびユーザを正常に認証できることを確認できます。

3. ***保存*をクリックします。**
   サーバーが*サーバー*リストに表示されます。
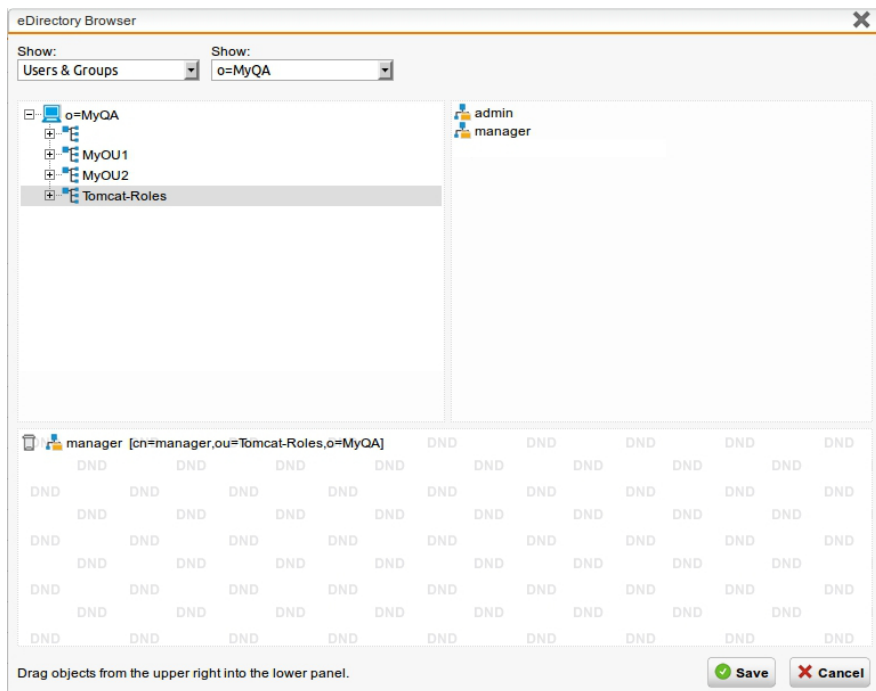
図 **17** グループ：Sophos UTMのeDirectoryブラウザ

5.6.2.2 Active Directory

Active Directory(AD)とは、マイクロソフトが実装したディレクトリサービスであり、Windows 2000/2003 Serverの中核を成すコンポーネントです。Active Directoryには、ユーザ、グループ、コンピュータ、プリンタ、アプリケーション、サービス、あらゆる種類のユーザ定義オブジェクトなど、ネットワーク内に存在するさまざまなリソースに関する情報が保存されます。このため、Active Directoryには、これらのリソースへのアクセスを一元的に体系化し、管理し、コントロールするための機能が用意されています。

Active Directory認証方式では、Sophos UTMをWindowsドメインに登録し、プライマリの*ドメインコントローラ*(DC)にSophos UTM用のオブジェクトを作成します。UTMは、このドメインのユーザとグループに関する情報を問い合わせることが可能になります。

注 – UTMはActive Directory 2003以降をサポートしています。

Active Directory認証を設定するには、次の手順に従ってください。

1. ***サーバ*タブで、*新規認証サーバ*をクリックします。**
   *認証サーバの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   バックエンド: バックエンドのディレクトリサービスとして*Active Directory*を選択します。

   位置 : バックエンドサーバの位置を選択します。番号が小さいバックエンドサーバから順に問い合わせが行われます。パフォーマンスを向上するためには、要求を最も多く受けると予想されるバックエンドサーバをリストの一番上に配置します。

   サーバ: Active Directoryサーバを選択または追加します。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

   SSL : SSLデータ転送を有効にするには、このオプションを選択します。すると、*ポート*が389(LDAP)から636(ldaps = LDAP over SSL)に変わります。

   ポート: Active Directoryサーバのポートを入力します。デフォルトで、ポート389が選択されています。デフォルトで、ポート389が選択されています。

   バインド**DN** : サーバにバインドするユーザの完全な*識別名*(DN)のLDAP表記法での指定。Active Directoryサーバへの匿名での問い合わせが許可されていない場合、このユーザが必要です。バインドユーザには、関連するすべてのユーザオブジェクト情報をActive

Directoryサーバから取得してユーザの認証を行うために必要な特権を付与する必要があります。通常は、ドメインの管理者がこの要件に対応します。

各DNは、Active Directoryユーザオブジェクトのいくつかの属性から成る1つ以上のRDN（*相対識別名*）で構成されます。ユーザ名、常駐するノード、サーバのトップレベルDNなどを、コンマ区切りのLDAP表記法で記述します。

- ユーザ名は、ディレクトリにアクセスできるユーザの名前にする必要があり、`CN`識別子（`CN=user`など）で指定します。ドメイン権限を持つ「admin」などの一般的なアカウントを使用することもできますが、ベストプラクティスとしては、admin権限を持たないユーザを指定することが推奨されます。この理由は、所与のベースDNを起点とするサブツリー内の全オブジェクトに対する読み取り権限さえあれば十分であるためです。
- ユーザオブジェクトが保存されているノードの情報には、ルートノードからユーザオブジェクトまですべてのサブノードが含まれている必要があり、通常はいわゆる*組織ユニット*コンポーネントや*一般名*コンポーネントから構成されます。組織ユニット（Microsoft Management Consoleでは、フォルダと本を組み合わせたアイコンで示される）は、識別子`OU`を使用して指定します。ノードは、最も低いノードから順に並べられ、末尾は最も高いノードになります。つまり、先頭は最も詳細な要素になります（例：`OU=Management_US,OU=Management`）。一方、事前定義されている*Users*ノードなどのデフォルトActive Directoryコンテナ（シンプルなフォルダアイコンで示される）は、識別子`CN`で指定します（例：`CN=Users`）。
- サーバのトップレベルDNは、それぞれ識別子`DC`で指定されている複数のドメインコンポーネントから構成することができます。ドメインコンポーネントはドメイン名と同じ順序で指定します（たとえば、ドメイン名がexample.comである場合、DN部分は`DC=example,DC=com`とします）。

たとえば、名前が`administrator`であり、オブジェクトが`example.com`ドメインの`Users`コンテナに保存されるバインドユーザのDNは次のようになります。

```
CN=administrator,CN=Users,DC=example,DC=com
```
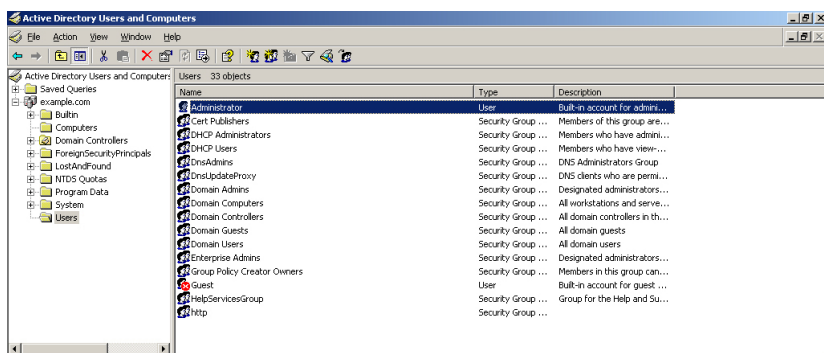
図 **18** 認証 : Microsoft Management Console

ここで、*Management*という名前の組織ユニットを作成し、サブノードを*Management_US*とし、管理者ユーザオブジェクトをこのサブノードに移動すると、管理者のDNは次のように変わります。`CN=administrator,OU=Management_US,OU=Management,DC=example,DC=com`

パスワード: バインドユーザのパスワードを入力します。

サーバ設定のテスト: *テスト*ボタンを押すと、設定されたサーバとのバインドテストが実行されます。これにより、このタブの設定が正しいこと、およびサーバーが起動しており、接続を受け付けていることが確認されます。

ベース**DN** : LDAPツリーのルートに相対的な開始位置で、ここに認証されるユーザが含まれています。ベース DN は、LDAP 表記の完全識別名 (FDN) で、コンマを区切り文字として使用して指定する必要があります (例: `O=Example,OU=RnD`)。ベースDNは空にすることもできます。この場合は、ベースDNは自動的にディレクトリから取り出されます。

ユーザ名 : 認証を実行するテストユーザのユーザ名を入力してください。

パスワード: テストユーザのパスワードを入力します。

サンプルユーザの認証 : *テスト*ボタンをクリックして、テストユーザの認証テストを開始します。これにより、すべてのサーバ設定が正しいこと、サーバが稼働中で接続を受け付けていること、およびユーザを正常に認証できることを確認できます。

3. ***保存*をクリックします。**
   サーバーが *サーバー*リストに表示されます。

ユーザプリンシパル名

場合により、資格情報を入力する際、ユーザはユーザプリンシパル名表記「user@domain」の使用が求められることがあります（例：Exchange ServerをActive Directoryサーバと組み合わせて使用する場合など）。

- 新規サーバを開始するには、希望するサーバに複製します。
- *バックエンド*から*LDAP*へ変更
- *ユーザ属性*から>へ変更
- *userPrincipalname*を*カスタム*フィールドに入力します。

まだ存在していない場合、これにより、「Active Directoryユーザ」グループの代わりに使用しなければならない「LDAPユーザ」グループを設定します。

注 – `domain\user`形式はサポートされていません。代わりに`user@domain`形式を使用します。

5.6.2.3 LDAP

LDAPとは、*Lightweight Directory Access Protocol*の略であり、X.500標準に基づいてディレクトリサービスの問い合わせと変更を行うネットワーキングプロトコルです。Sophos UTMでは、複数のサービスへのユーザ認証にLDAPプロトコルを使用しており、LDAPサーバに設定された属性やグループメンバシップに基づいてアクセスを許可または却下します。

LDAP認証を設定するには、次の手順に従ってください。

1. ***サーバ*タブで、*新規認証サーバ*をクリックします。**
   *認証サーバの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   バックエンド: バックエンドのディレクトリサービスとして*LDAP*を選択します。

   位置：バックエンドサーバの位置を選択します。番号が小さいバックエンドサーバから順に問い合わせが行われます。パフォーマンスを向上するためには、要求を最も多く受けると予想されるバックエンドサーバをリストの一番上に配置します。

   サーバ: LDAPサーバを選択または追加します。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

SSL：SSLデータ転送を有効にするには、このオプションを選択します。すると、*ポート*が389（LDAP）から636（ldaps＝LDAP over SSL）に変わります。

ポート: LDAPサーバのポートを入力します。デフォルトで、ポート389が選択されています。

バインド**DN**：サーバにバインドするユーザの*識別名*（DN）を指定します。このユーザは必須です。セキュリティ上の理由から、LDAPサーバへの匿名での問い合わせはサポートされていません。このユーザには、関連するすべてのユーザオブジェクト情報をLDAPサーバから取得してユーザを認証するために必要な特権が付与されている必要があります。LDAPユーザ、グループ、コンテナは、LDAP表記法で完全識別名として指定します。区切り文字にはコンマを使用します。
（例：CN=administrator,DC=intranet,DC=example,DC=com）

パスワード: バインドユーザのパスワードを入力します。

サーバ設定のテスト: *テスト*ボタンを押すと、設定されたサーバとのバインドテストが実行されます。これにより、このタブの設定が正しいこと、およびサーバーが起動しており、接続を受け付けていることが確認されます。

ユーザ属性：LDAPディレクトリ検索用のフィルタとして使用されるユーザ属性を選択します。ユーザ属性には、リモートアクセスサービスなどが各ユーザに対してプロンプト表示する実際のログイン名が含まれます。次のユーザ属性を選択できます。

- CN（一般名）
- SN（名字）
- UID（ユーザID）

LDAPディレクトリのユーザ名がこれらのフォームに保存されていない場合、リストで*カスタム* *<<Custom>>* を選択し、下の*カスタム* *Custom* フィールドにカスタム属性を入力します。この属性はLDAPディレクトリで設定する必要があります。

ベース**DN**：LDAPツリーのルートに相対的な開始位置で、ここに認証されるユーザが含まれています。ベース DN は、LDAP 表記の完全識別名（FDN）で、コンマを区切り文字として使用して指定する必要があります（例: O=Example,OU=RnD）。ベースDNは空にすることもできます。この場合は、ベースDNは自動的にディレクトリから取り出されます。

ユーザ名：認証を実行するテストユーザのユーザ名を入力してください。

パスワード: テストユーザのパスワードを入力します。

サンプルユーザの認証：*テスト*ボタンをクリックして、テストユーザの認証テストを開始します。これにより、すべてのサーバ設定が正しいこと、サーバが稼働中で接続を受け付けていること、およびユーザを正常に認証できることを確認できます。

3. ***保存*をクリックします。**
   サーバーが *サーバー*リストに表示されます。

5.6.2.4 RADIUS

RADIUSとは、*Remote Authentication Dial In User Service*の略であり、ルータなどのネットワークデバイスで中央データベースに対してユーザを認証するために広く用いられているプロトコルです。RADIUSには、ユーザの情報に加え、ネットワークデバイスで使用される技術情報（サポートされるプロトコル、IPアドレス、ルーティング情報など）も保存できます。この情報は、RADIUSサーバ上のファイルまたはデータベースに保存されるユーザプロファイルを構成します。

RADIUSプロトコルは非常に柔軟であり、サーバはほとんどのオペレーティングシステムで利用可能です。UTMにRADIUSを導入することで、プロキシとユーザに基づいてアクセス権限を設定できるようになります。RADIUS認証を使用するためには、ネットワーク上で稼働しているRADIUSサーバが必要です。パスワードはRADIUS シークレットを使用して暗号化されますが、ユーザ名は平文の形で伝送されます。

RADIUS認証を設定するには、次の手順に従ってください。

1. ***サーバ*タブで、*新規認証サーバ*をクリックします。**
   *認証サーバの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   バックエンド：バックエンドのディレクトリサービスとして*RADIUS*を選択します。

   位置：バックエンドサーバの位置を選択します。番号が小さいバックエンドサーバから順に問い合わせが行われます。パフォーマンスを向上するためには、要求を最も多く受けると予想されるバックエンドサーバをリストの一番上に配置します。

   サーバ：RADIUSサーバを選択または追加します。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

   ポート：RADIUSサーバのポートを入力します。デフォルトで、ポート`1812`が選択されています。

   共有シークレット：共有シークレットとは、RADIUSクライアントとRADIUSサーバの間でパスワードとしての役割を果たすテキスト文字列です。共有シークレットを入力します。

サーバ設定のテスト: *テスト*ボタンを押すと、設定されたサーバとのバインドテストが実行されます。これにより、このタブの設定が正しいこと、およびサーバーが起動しており、接続を受け付けていることが確認されます。

ユーザ名 : 認証を実行するテストユーザのユーザ名を入力してください。

パスワード: テストユーザのパスワードを入力します。

NAS識別子 : 適切なNAS識別子をリストから選択します。詳細は、注記と下の表を参照してください。

サンプルユーザの認証 : *テスト*ボタンをクリックして、テストユーザの認証テストを開始します。これにより、すべてのサーバ設定が正しいこと、サーバが稼働中で接続を受け付けていること、およびユーザを正常に認証できることを確認できます。

3. ***保存*をクリックします。**
サーバーが *サーバー*リストに表示されます。

注 – RADIUSサーバに問い合わせを行う、Sophos UTMの各ユーザ認証サービス(PPTPやL2TP)は、異なる識別子(NAS識別子)をRADIUSサーバに送信します。たとえば、PPTPサービスは、このユーザの認証を試みるときに、pptpというNAS識別子をRADIUSサーバに送信します。これにより、RADIUSサーバがさまざまなサービスを識別して特定の種類のサービスをユーザに付与することができるため、権限付与の目的で役に立ちます。ユーザ認証サービスとそれに対応するNAS識別子のリストは以下のとおりです。

ユーザ認証サービス	**NAS**識別子
SSL VPN	ssl
PPTP	pptp
IPsec	ipsec
L2TP over IPsec	l2tp
SMTPプロキシ	smtp
ユーザポータル	portal
WebAdmin	webadmin

ユーザ認証サービス	NAS識別子
ソックスプロキシ	socks
Webフィルタ	http
認証クライアント	agent
ワイヤレスアクセスポイント	NAS IDはワイヤレスネットワーク名です。

表1: RADIUS NAS識別子

5.6.2.5 TACACS+

TACACS+(*Terminal Access Controller Access Control System*の略語)とは、Cisco Systems, Inc.独自のプロトコルであり、認証プロセスと権限付与プロセスについて詳細なアカウンティング情報と管理的なコントロールを提供します。RADIUSでは認証と権限付与がユーザプロファイルにまとめられていますが、TACACS+ではこれらのオペレーションを区別しています。他の相違点としては、TACACS+ では TCP プロトコル (ポート 49)を使用し、RADIUS では UDP プロトコルを使用します。

TACACS+認証を設定するには、次の手順に従ってください。

1. ***サーバ*タブで、*新規認証サーバ*をクリックします。**
   *認証サーバの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   バックエンド: バックエンドのディレクトリサービスとして*TACACS+*を選択します。

   位置 : バックエンドサーバの位置を選択します。番号が小さいバックエンドサーバから順に問い合わせが行われます。パフォーマンスを向上するためには、要求を最も多く受けると予想されるバックエンドサーバをリストの一番上に配置します。

   サーバ: TACACS+サーバを選択または追加します。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

   ポート: TACACS+サーバのポートを入力します。デフォルトで、ポート49が選択されています。

   鍵 : Sophos UTMとTACACS+サーバの間のすべてのTACACS+通信に使用する認証および暗号鍵を入力します。ここで入力する鍵の値は、TACACS+サーバで設定した値と一致している必要があります。鍵を入力してください(確認のために2回)。

サーバ設定のテスト: *テスト*ボタンを押すと、設定されたサーバとのバインドテストが実行されます。これにより、このタブの設定が正しいこと、およびサーバーが起動しており、接続を受け付けていることが確認されます。

ユーザ名：認証を実行するテストユーザのユーザ名を入力してください。

パスワード: テストユーザのパスワードを入力します。

サンプルユーザの認証：*テスト*ボタンをクリックして、テストユーザの認証テストを開始します。これにより、すべてのサーバ設定が正しいこと、サーバが稼働中で接続を受け付けていること、およびユーザを正常に認証できることを確認できます。

3. ***保存*をクリックします。**
サーバーが *サーバー*リストに表示されます。

5.6.3 シングルサインオン

定義とユーザ > *認証サービス* > *シングルサインオン*タブでは、Active DirectoryまたはeDirectory（あるいはその両方）のシングルサインオン機能を設定できます。

Active Directoryのシングルサインオン(SSO)

Active DirectoryのSSO機能は現在、Webフィルタのみで使用されており、NTLMv2またはKerberos認証をサポートするブラウザでシングルサインオン機能を使用できます。

シングルサインオン機能を有効にするには、UTMをActive Directoryドメインに追加する必要があります。追加するドメインが機能するためには、次の前提条件を満たしている必要があります。

- ゲートウェイのクロックとDCのクロックの間に、5分を超える時刻差がない。
- UTMホスト名がADDNSシステムに存在する。
- UTMAD DNSをフォワーダとして使用しているか、ADドメインのDNS要求ルートがAD DNSサーバをポイントしている。

注 – Active Directoryグループメンバシップ同期では、シングルサインオン（SSO）パスワードを使用してADサーバーと通信します。このパスワードを変更する場合、新規パスワードを入力して、UTMをもう一度サーバに同期させるためUTMを再参加させる必要があります。

Active Directory SSOを設定するには、次の手順に従ってください。

1. **Active Directory**サーバを*サーバ*タブで作成します。
2. **次の設定を行います。**

ドメイン: ドメインの名前(`intranet.mycompany.com`など)。UTMはDNSを使用して取得可能なすべてのDCを検索します。

adminユーザ名 : 管理者権限があり、ドメインにコンピュータを追加することが許可されているユーザ(通常は「管理者」)。

パスワード: adminユーザのパスワード。

3. ***適用*をクリックします。**
設定が保存されます。

Kerberos認証サポートに関する注記 : SSO Kerberosサポートが機能するためには、クライアントはプロキシ設定でUTMのFQDNホスト名を使用する必要があります。IPアドレスを使用すると機能しません。NTLMv2モードは、この要件の影響を受けません。この要件が満たされていない場合や、ブラウザがKerberos認証をサポートしない場合には、NTLMv2モードが自動的に使用されます。

eDirectoryのシングルサインオン SSO

ここでは、eDirectory用にSSOを設定できます。*Webプロテクション* > *Webフィルタリング*で認証方式として*eDirectory SSO*を設定した場合、ここで選択したeDirectoryサーバが使用されます。

eDirectory SSOを設定するには、次の手順に従ってください。

1. **eDirectoryサーバを*サーバ*タブに登録します。**

2. **次の設定を行います。**
サーバ: SSOを有効にするeDirectoryサーバ。

同期間隔 : UTMとeDirectoryサーバ間での同期イベントの間隔(秒数)。

3. ***適用*をクリックします。**
設定が保存されます。

5.6.4 ワンタイムパスワード

定義とユーザ > *認証サービス* > *ワンタイムパスワード*タブで、ワンタイムパスワード(OTP)サービスを設定し、ワンタイムパスワードユーザのトークンを監視または編集することができます。ワンタイムパスワードは、パスワードベースの認証のセキュリティを向上できる方法です。時には弱すぎるユーザ独自のパスワードが、一度のログインでのみ有効なワンタイムパスワードによって修正されます。したがって、たとえ攻撃者がパスワードを入手しても、それでログインすることはできません。

ワンタイムパスワードは、特定のアルゴリズムによる計算で、常に定期的に変更されます。新しいパスワードが計算されると、古いパスワードは自動的に有効期限が切れます。ワンタイムパスワードを計算するには、該当するソフトウェアが搭載されているモバイルデバイスか、特殊なハードウェアまたはセキュリティトークンが必要になります。ハードウェアトークンはすぐに使えます。モバイルデバイスの場合は、ユーザポータルのスタートページまたは*OTP トークン*ページ(*ユーザポータル*ページを参照)でQRコードとして入手できるGoogle認証システムまたは類似のソフトウェアをインストールして、設定を行う必要があります。この作業を完了すると、デバイスはトークンに固有の間隔でワンタイムパスワードを計算します。ワンタイムパスワードの生成ではタイムスタンプを使用するので、日付と時刻が正確であることが重要です。

注 – ワンタイムパスワードが必要な機能で認証を行うには、ユーザに固有のUTMパスワードに続けて、すぐにワンタイムパスワードを入力する必要があります。

また、管理者が手動で、パスコードと呼ばれるワンタイムパスワードを生成することも可能です。この場合、この時間が限定されないワンタイムパスワードが、必ず安全にエンドユーザに転送されることを確認する必要があります。ただし、このプロセスは、たとえばユーザが一時的にパスワード計算デバイスにアクセスできない場合など、あくまでも暫定的な解決策と考えるべきです。

注 – ワンタイムパスワードが必要な機能で認証を行うには、ユーザに固有のパスワードに続けて、すぐにワンタイムパスワードを入力する必要があります。また、管理者が手動で、パスコードと呼ばれるワンタイムパスワードを生成することも可能です。

ワンタイムパスワードサービスの有効化と設定

ワンタイムパスワードサービスを設定するには、以下の手順に従います。

1. ***OTP設定 セクション*で、以下の設定を行います。**
   すべてのユーザがワンタイムパスワードを使用:デフォルトでは、このチェックボックスが有効であり、すべてのユーザがワンタイムパスワードを使用しなければなりません。特定のユーザだけがワンタイムパスワードを使用しなければならない場合は、このチェックボックスを無効にして、ユーザまたはグループを選択するか、ボックスに追加します。

   警告 – *すべてのユーザがワンタイムパスワードを使用*の機能を無効にすると、自動的にUTMの別の部分の*ユーザ/グループ*に影響が出ます。例えば、*リバース認証*に影響が出ます。

注 – バックエンド認証ののユーザについては、*自動的にユーザを作成*オプションを有効にしなければなりません。オプションは、*定義とユーザ* > *認証サービス* > *グローバル設定* > *自動ユーザ作成*で確認できます。

ユーザの**OTP**トークンを自動作成：これを選択すると、許可されたユーザが次回ユーザポータルにログインした時に、モバイルデバイス用ソフトウェアを設定するためのQRコードが提示されます。これが機能するために、ユーザがユーザポータルにアクセスできることを確認してください（*マネジメント* > *ユーザポータル*ページを参照）。ユーザがユーザポータルにログインすると、それぞれのトークンが*OTP トークン*リストに表示されます。モバイルデバイスで、ソフトトークンを使用する場合、この機能を有効にすることを推奨いたします。ユーザがハードウェアトークンだけを使用する場合は、このチェックボックスを無効にし、OTP機能を有効にする前にトークンを追加またはインポートします。

機能に対して**OTP**を有効にする：ここで、UTM選択したユーザがワンタイムパスワードによってアクセスする必要がある機能を選択します。*ユーザのOTP トークンを自動作成*チェックボックスを選択する場合、セキュリティ上の理由から、ユーザポータルが有効である必要があります。これは、ユーザポータルはOTPトークンへのアクセスを与えるので、それ自体に保護が弱い部分があってはならないからです。安全なシェルアクセスのOTPを有効にするには、それぞれのトークンについて追加的にシェルアクセスの使用を有効にする必要があります（手動でのOTPトークンの追加または編集を参照）。これで、該当するユーザは、ワンタイムパスワードが追加されたログインユーザパスワードで*ログインユーザ*としてログインしなければならなくなります。

警告 – 特に、OTPでの使用のためにWebAdminまたはシェルアクセスを選択する場合、選択したユーザがワンタイムパスワードのトークンにアクセスできることを確認しなければなりません。そうしないと、それらのユーザは永続的にログアウトしたままになります。

2. *タイムステップ設定*セクションで、以下の設定を行います。
   デフォルトのトークンのタイムスタンプ：モバイルデバイスとでワンタイムパスワードを同期させるにはUTM、両方のタイムスタンプが同一でなければなりません。一部のハードウェアトークンは、60秒を使用します。別のソフトウェアOTPトークンは30秒のステップを使用し、ここではそれがデフォルト値となっています。タイムスタンプが一致しなければ、認証は失敗します。ここで入力する値は、自動的にそれぞれの新しいOTPトークンで使用されます。許可されているタイムステップの範囲は、10～120です。

最大パスコードオフセット: このオプションにより、最大パスコードオフセットステップを設定可能です。例えば3ステップに設定した場合、2回のログインの間にタイムステップ数3を超えてドリフトしないよう、トークンのクロックが制限されます。最大パスコードオフセットは、0～10の範囲でなければなりません。

最大初期パスコードオフセット: このオプションにより、最大初期パスコードオフセットステップを設定可能です。例えば10ステップに設定した場合、2回のログインの間にタイムステップ数10を超えてドリフトしないよう、トークンのクロックが制限されます。最大初期パスコードオフセットは、0～600の範囲でなければなりません。

3. ***適用*をクリックします。**
設定が保存されます。

4. **ハードウェアトークンを使用する場合、それらを*OTP トークン*セクションにインポートまたは追加します。**
右上のインポートアイコンをクリックします。*CSVインポート*方式を選択します。そして、CSV区切りデータをテキストボックスに貼り付け、*保存*をクリックします。

PSKC *アップロード*: OATH-TOTP規格を使用するOTPトークンは主に、PSKCフォーマットを使用するシリアル番号およびシークレットを含むファイル内で生成されます。暗号化ファイルについては、復号化キーが帯域外（紙ベース）で供給されます。

右上のインポートアイコンをクリックします。*PSKC アップロード*方式を選択します。ファイルを選択し、*アップロード開始*をクリックします。ファイルが暗号化されている場合、*復号化キー*を入力して*保存*をクリックします。

CSV*インポート*: ハードウェアトークンのベンダーから受け取ったデータを使用して、UTF-8エンコーディングでセミコロンを使用する、CSVファイルを生成します。このファイルには3つの列、シークレット、タイムステップ、コメントが含まれていなければなりません。デバイスに固有の一意の文字列であるシークレットは必須であり、16進フォーマットで、長さは128ビットです。他の列は、空白です。タイムステップが空白であると、*OTP設定*セクションで定義されたデフォルトのトークンのタイムステップが使用されます。

インポート/アップロードすると、編集アイコンを使用して変更することができます。さらに、プラス「+」アイコンをクリックすると、いつでも単一のエントリを追加できます（手動でのOTPトークンの追加または編集を参照）。

5. **ワンタイムパスワードサービスを有効にする。**
ページ上部にあるトグルスイッチをクリックします。トグルスイッチが緑色に変わります。

*ユーザのOTPトークンを自動作成*が有効であれば、ワンタイムパスワードによる認証を指定されたユーザが初めてユーザポータルにログインした時に、まだ生成されていなければ、UTMOTPトークンのエントリを自動作成します。加えて、エントリの*リセット*アイコンが有効になります。

エントリのトグルスイッチを使用すると、たとえばユーザがハードウェアトークンを紛失した場合などに、無効にすることができます。該当するアイコンを使用して、たとえばハードウェアトークンが破損した場合などに、削除することができます。どちらのケースでも、*ユーザのOTPトークンを自動作成*オプションが有効であれば、トークンのシークレットにアクセスできるので、引き続き再認証が可能です。*OTPトークン*リストに、新しいエントリが表示されます。

*OTPトークン*リストの右上では、検索ボックスとナビゲーションアイコンを使用してリストのナビゲーションやフィルタを行うことができます。

アイコン

OTPトークンエリアに、追加の機能アイコンがいくつかあります。

機能アイコン	意味
	トークンを「まったく使用されない」状態、すなわち初期状態に設定します。リセットを実行すると、ユーザポータルにロギングした時に再度QRコードが表示されます。リセット機能は、ユーザが少なくとも1回OTPでログインした場合に利用可能です。
	トークンがリモートシェルアクセスに使用するよう設定されていることを示します。
	トークン情報がユーザポータルに非表示であることを示します。
	追加のトークンコードを示します。
	トークンタイムオフセットを示すことが可能となります。
	トークンのQRコードとその情報を示します。

OTPトークンを手動で追加または編集する

OTPトークンを追加または編集することができます。

ヒント – 通常、単一のOTPトークンを追加することはありませんが、ハードウェアトークンであればインポートすることができますし、モバイルデバイスを使用している場合は、*ユーザのOTPトークンを自動作成* *Auto-create OTP tokens for users* オプションを使用して自動的に生成することができます。

1. **ダイアログを開いて、OTPトークンを追加または編集します。**
   OTPトークンを追加するには、*OTP トークン*リストの右上にある緑のプラス「+」アイコンをクリックします。

   OTPトークンを編集するには、*OTP トークン*リストのそれぞれのエントリの前にある編集アイコンをクリックします。

2. **次の設定を行います。**
   ユーザ：トークンを割り当てるユーザを選択または追加します。

   シークレット：これは、ユーザのハードウェアトークンまたはソフトトークンの共有シークレットです。ハードウェアトークンには、ハードウェアの製造会社によって与えられた変更できないシークレットがあります。*ソフトトークンは*、*ユーザのOTP トークンを自動作成*が有効である場合に、UTMによってランダムに作成されます。シークレットは、長さ128ビットの16進フォーマットである必要があります。

   コメント(オプション)：説明などの情報を追加します。このテキストは、ユーザポータルでQRコードと共に表示されます。ある人に異なるトークン（例、ハードウェアトークンおよび携帯電話用ソフトトークン）を定義する場合、ユーザにはすべてのQRコードが並んで表示されるので、何らかの説明を入力しておくと便利です。

3. **次の詳細設定を任意で行います。**
   *カスタム トークンのタイム ステップ*を使用：トークンに対して、*OTP設定*セクションで定義されたデフォルトのトークンタイムステップ以外のタイムステップが必要であれば、このチェックボックスを有効にして、値を入力します。ここで定義するタイムステップは、ユーザのパスワード生成用デバイスのタイムステップと対応している必要があり、対応していない場合、認証が失敗します。

   ユーザ ポータルで トークン情報 を非表示 にする：これを有効にすると、トークンはユーザポータルで非表示になります。これは、たとえば設定が必要ではないハードウェアトークンや、たとえばソフトトークンの設定をエンドユーザではなく、管理者によって集中的に設定するべき場合に便利です。

   トークンはシェルアクセスで使用可能：これを有効にすると、UTMに対するコマンドラインアクセスでトークンを使用できるようになります。これが機能するために、*OTP設定*セクションでシェルアクセスが有効で、に対して一般にパスワード認証によるシェルアクセスが有効である必要がありますUTM（*マネジメント*> *システム設定* > *シェルアクセスを参照*）。シェルアクセス権限があるOTPトークンには、右側にコマンドシェルアイコンがあります。ワンタイムパスワードによるシェルアクセスの場合、これで該当するユーザは、ワンタイムパスワードが

追加されたログインユーザパスワードで*ログインユーザ*としてログインしなければならなくなります。

追加コード(OTPトークンの編集の場合のみ):手動で、トークンに対してワンタイムパスワードを追加することができます。緑のプラス「+」アイコンをクリックして、一度にワンタイムパスワードを入力するか、*生成*ボタンを使って、一度に10のワンタイムパスワードを生成します。また、アクションアイコンを使用して、ワンタイムパスワードのインポートやエクスポートを行うことも可能です。こうしたワンタイムパスワードは、時間が限定されません。ワンタイムパスワードを使ってユーザがログインすると、ワンタイムパスワードは自動的に削除されます。追加のワンタイムパスワードがあるOTPトークンには、右側にプラス「+」アイコンがあります。そのアイコンの上へカーソルを移動させると、ワンタイムパスワードのリストが表示されます。

4. ***保存*をクリックします。**
   設定が保存されます。

OTPトークンタイムの同期

ハードウェアOTPトークンの場合、それらの内蔵水晶クロックが「実際の」クロックより、遅くなるまたは早まる可能性があります。例えば、VASCOトークン仕様では、毎日約2秒のタイムドリフトが許可されています。数カ月後に、ハードウェアトークンのタイムドリフトが大きくなり、トークンのOTPコードがUTMの算出OTPに一致しなくなる可能性があります。また、1トークンコードをプラス/マイナスしたデフォルト認可OTPウィンドウに一致しないほど、高くなる場合があります。その場合、OTPコードはUTMにより否認されます。

毎回ユーザが有効なハードウェアトークンコードを使用してUTMにログオンするたびに、UTMはそのトークンコードがワンタイムステップ値を超えているかどうかを計算します。超えている場合、UTMはトークン固有のタイムドリフト値を自動的に変更します。

UTMにより、タイムオフセットを計算し同期できます。次の手順で実行します。

1. **OTPトークンエリアで、ストップウォッチのアイコンをクリックします。**
   「OTPトークンタイムオフセットをチェック」ダイアログボックスが開きます。このトークンの現在のオフセットが表示されます。

2. ***トークンパスコード*を入力します。**
   トークンパスコードは、ハードウェアデバイスにより生成された6桁の番号です。

3. ***チェック*をクリックします。**
   数秒後に結果が表示されます。パスコードが有効である場合、メッセージによりトークンがオフであるか、およびタイムステップ回数が示されます。

4. **そのトークンのオフセットを設定する場合は、*OK*をクリックします。**
   トークンタイムオフセットがアップデートされます。

5. *キャンセル***をクリックします。**
   ダイアログボックスが閉じます。

5.6.5 詳細

パスワード推測のブロック

この機能を使用してパスワードが推測されないようにします。設定した回数のログインに失敗すると(デフォルトでは:3回)、機能へのアクセスを取得しようとしているIPアドレスは設定した時間(デフォルトでは:600秒間)ブロックされます。

ブロックされているホストからのパケットをドロップする:これを有効にすると、ブロックされているホストからのすべてのパケットが、指定された時間の間ドロップされます。このオプションは、DoS攻撃を回避するために使用されます。

機能:チェックすると、選択した機能に対して実行されます。

ブロック対象外ネットワーク:このボックスにリストされているネットワークは、このチェックから除外されます。

ローカル認証パスワード

このオプションを使用すると、管理者や管理者権限を持つローカル登録ユーザに対して、パスワードの強化を強制できます。次のセキュリティ要件を遵守するパスワードの複雑性を設定できます。

- パスワードの最低長。デフォルトは8文字
- 小文字が1つ以上必要
- 大文字が1つ以上必要
- 数字が1つ以上必要
- 英数字以外の文字が1つ以上必要

選択したパスワードプロパティを有効にするためには、*複雑なパスワードを必須にする*チェックボックスにチェックを入れて、*適用*をクリックします。

Active Directoryグループメンバシップの同期

このオプションを使用し、ADグループメンバシップ情報のバックグラウンド同期を有効にします。

UTMは、グループメンバシップ情報を定期的に同期化し、Active Directoryサーバへのトラフィックを軽減するため、ローカルでキャッシュに格納します。このオプションが有効な場合、グループメンバシップ情報は設定されたActive Directoryのシングルサインオンサーバとともに同期化されます。

*すぐに同期化*をクリックして、即時にグループメンバシップ情報を同期化します。

ディレクトリユーザのプリフェッチ

eDirectoryまたはActive DirectoryのユーザをUTMと同期することができます。これにより、UTMにユーザーオブジェクトが事前に作成され、当該ユーザーがログインしたときには、これらのユーザーオブジェクトがすでに存在しています。同期プロセスは週次または日次で実行できます。

プリフェッチを有効にするには、次の設定を行います。

サーバ:ドロップダウンリストには、*サーバ*タブで作成されたサーバが含まれています。プリフェッチを有効にするサーバを選択します。

プリフェッチ間隔: ユーザをプリフェッチする間隔を選択します。同期を週次で実行する場合、同期を開始する曜日を選択します。同期を日次で実行する場合、*デイリー*を選択します。

プリフェッチ時刻:ユーザをプリフェッチする時刻を選択します。

グループ:どのグループを事前に作成するか指定するには、ここでグループを入力します。統合LDAPブラウザを使用して、これらのグループを選択できます。

ログイン時のバックエンド同期を有効化(オプション):すべてのプリフェッチイベントで、関与するユーザ(*ユーザとグループ* > *ユーザ*タブ)の*バンクエンドの同期*オプションは、ここで定義する値に設定されます。このオプションを有効にした場合、ユーザの*バンクエンドの同期*オプションが有効になります。このオプションを無効にした場合は、*バンクエンドの同期*オプションが無効になります。

設定を保存するには*適用*をクリックします。

直ちにプリフェッチ: プリフェッチを今すぐ開始するには、このボタンをクリックします。

プリフェッチライブログを開く: プリフェッチのライブログを開くには、このボタンをクリックします。

6 インタフェースとルーティング

この章では、Sophos UTMでインタフェースとネットワーク固有の設定を構成する方法について説明します。WebAdminの*ネットワーク統計*ページには、今日の上位 10件のアカウンティングサービス、上位送信元ホスト、および同時接続の概要が表示されます。各セクションには*詳細*リンクがあります。リンクをクリックするとWebAdminのそれぞれのレポーティングセクションが表示され、そこでさらなる統計情報を参照できます。

この章には次のトピックが含まれます。

- インタフェース
- ブリッジ
- QoS
- アップリンクモニタリング
- IPv6
- スタティックルート
- OSPF
- BGP
- マルチキャストルーティング(PIM-SM)

6.1 インタフェース

ゲートウェイには、内部LANを外部ネットワーク(インターネットなど)にセキュリティを維持して接続するために、少なくとも2つのネットワークインタフェースカードが必要です。次の例では、ネットワークカード eth0 は、常に、内部ネットワークに接続されるインタフェースです。一方、ネットワークカード eth1 は、外部ネットワーク(インターネットなど)に接続されるインタフェースです。これらのインタフェースは、それぞれ信頼されるインタフェース、信頼されないインタフェースとも呼ばれます。

ネットワークカードは、インストール中に自動認識されます。ソフトウェアアプライアンスでは、新しいネットワークカードを後で追加すると、新たなインストールが必要になります。システムの再インストールを行うには、設定のバックアップを作成し、ソフトウェアをインストールし、バックアップを復元するだけです。

内部ネットワークと外部ネットワークの接点は、ゲートウェイのみであるようにしてください。すべてのデータは UTM を通過する必要があります。内部インタフェースと外部インタフェースを 1つのハブ

またはスイッチに接続することは推奨しません。ただし、スイッチが、VLAN スイッチとして設定されている場合は除きます。誤った ARP（アドレス解決プロトコル）解決が発生する可能性があり、これを「ARP クラッシュ」と呼びます。この状況は、（マイクロソフト製品など）OS によっては管理できないものもあります。このため、各ゲートウェイネットワークインタフェースに対して、1つの物理ネットワークセグメントを使用する必要があります。

*インタフェース*メニューでは、UTM にインストールされているすべてのネットワークカードを設定・管理したり、外部ネットワーク（インターネット）へのすべてのインタフェースや内部ネットワーク（LAN、DMZ）へのインタフェースを設定・管理したりすることができます。

注 - ネットワークトポロジを計画し、UTM を設定しているときは、どのインタフェースがどのネットワークに接続しているかに注意してください。ほとんどの設定で、SysIDが`eth1`のネットワークインタフェースは外部ネットワークへの接続として選択されます。冗長化（HA）フェイルオーバーをインストールするためには、同じ SysID のネットワークカードを両システムで選択する必要があります。HA フェイルオーバーのインストールについて詳細は、*管理* > *冗長化*のページを参照してください。

次のセクションでは、*インタフェース*、*追加アドレス*、*リンクアグリゲーション*、*アップリンクバランス*、*マルチパスルール*、*ハードウェア*のタブで、さまざまなインタフェースタイプを管理・設定する方法について説明します。

6.1.1 インタフェース

*インタフェース*タブでは、ネットワークカードと仮想インタフェースを設定できます。リストに、すでに定義されているインタフェースが、シンボル名、ハードウェアデバイス、現在のアドレスとともに表示されます。インタフェースのステータスも表示されます。トグルスイッチをクリックして、インタフェースを有効または無効にすることができます。インタフェースグループにはトグルスイッチがないことに注意してください。

ヒント – *インタフェース*リストでインタフェース定義の情報アイコンをクリックすると、インタフェース定義が使用されているすべての設定オプションを表示することができます。

新たに追加されたインタフェースは、セットアップ中、*ダウン*と表示される可能性があります。対応するボタンをクリックして、インタフェースを編集したり削除することができます。

6.1.1.1 自動インタフェースネットワーク定義

UTM の各インタフェースには、シンボル名とハードウェアデバイスが割り当てられています。シンボル名は、他の構成設定でインタフェースを参照するときに使用します。各インタフェースについて、次のような対応するネットワーク定義のセットが UTM によって自動的に作成されます。

- インタフェースの現在の IP アドレス、およびインタフェース名と *(アドレス)* サフィックスから成る名前が含まれる定義。
- インタフェースに接続されたネットワーク、およびインタフェース名と *(ネットワーク)* サフィックスから成る名前が含まれる定義。この定義は、*PPP* タイプのインタフェースに対しては作成されません。
- インタフェースのブロードキャストアドレス、およびインタフェース名と *(ブロードキャスト)* サフィックスから成る名前が含まれる定義。この定義は、*PPP* タイプのインタフェースに対しては作成されません。

インタフェースで動的アドレス割り当て方法 (DHCP やリモート割り当てなど) が使用されている場合、これらの定義は自動的に更新されます。ファイアウォールや NAT ルールなど、これらの定義を参照するすべての設定も、変更されたアドレスで自動的に更新されます。

Internal(内部) というシンボル名のインタフェース 1つが事前に定義されています。これは管理用インターフェースであり、通常、「内部」UTM インタフェースとして使用されます。名前を変更したい場合は、インストール直後に行う必要があります。

6.1.1.2 インタフェースタイプ

UTMに追加可能なインタフェースの種類と、それをサポートするために必要なハードウェアの種類は次のとおりです。

グループ: インタフェースをグループに編成することができます。これにより、該当する構成では、複数のインタフェースを個別に選択する代わりに、1つのインタフェースグループを選択できるようになります。

3G/UMTS: これは、USBモデムスティックに基づくインタフェースです。インタフェースを作成する前に、モデムスティックを差し込み、UTMを再起動する必要があります。

DSL PPPoA/PPTP : PPP over ATM。DSL PPPoAデバイスでは、ゲートウェイを*PPP-over-ATM*互換のDSL回線に接続できます。これらのデバイスは、PPTPプロトコルを使用してIPパケットをトンネリングします。これらのデバイスには専用イーサネット接続が必要です (同じハードウェア上で他のインタフェースと共存できません)。DSLモデムをインタフェースネットワークセグメントに接続する必要があります。これらのデバイスタイプのネットワークパラメータは、リモートステーションで割

り当てることができます(一般的にはご利用のISP)。さらに、ISPアカウントのユーザ名およびパスワードを入力する必要があります。また、お使いのモデムのIPアドレスも入力する必要があります。このアドレスは通常モデムに組み込まれているため変更できません。モデムで通信するには、NIC IPアドレスとネットマスクを入力する必要があります。モデムのIPアドレスは、これらのパラメータで定義されたネットワーク内であることが必要です。*Ping先アドレス*は、ICMP ping要求に応答するPPTPリンクの反対側のホストである必要があります。ご利用のISPのDNSサーバを使用することができます。このアドレスでpingできなかった場合、接続がデッド(dead)であることが考えられ、これは再開されます。

DSL PPPoE：PPP over Ethernet。DSL PPPoEデバイスでは、ゲートウェイを*PPP-over-Ethernet*互換のDSL回線に接続できます。これらのデバイスには専用イーサネット接続が必要です(同じハードウェア上で他のインタフェースと共存できません)。DSLモデムをインタフェースネットワークセグメントに接続する必要があります。これらのデバイスタイプのネットワークパラメータは、リモートステーションで割り当てることができます(一般的にはご利用のISP)。さらに、ISPアカウントのユーザ名およびパスワードを入力する必要があります。

イーサネット**DHCP**:これはDHCPを使用した標準イーサネットインタフェースです。

イーサネット:これは標準のイーサネットインターフェースで、10、100、あるは1000Mbpsの帯域幅を備えています。

イーサネット**VLAN**:VLAN(仮想LAN)は単一のハードウェアインタフェース上に別個のレイヤ2ネットワークセグメントを複数持つ方式です。各セグメントは整数の「タグ」で識別されます。VLANインタフェースを追加することで、インタフェース(エイリアス)の追加に使用できる「ハードウェア」デバイスが作成されます。PPPoEおよびPPPoAデバイスはVLAN仮想ハードウェア上では実行できません。

モデム **PPP**：UTMこのタイプのインタフェースでは、PPPモデムを介してをインターネットに接続できます。設定には、UTMにシリアルインタフェースと外部モデムが必要です。また、ユーザ名とパスワードを含むDSLアクセスデータも必要です。これらのデータはISPから入手できます。

フレキシブルスロットについて

一部のSophosハードウェアアプライアンスにあるスロットを使用して、容易にハードウェアインタフェースを変更することができます。スロットモジュールを挿入し、柔軟に切り替えることができます。そのようなハードウェアを使用している場合、WebAdminでは、各ハードウェアインターフェースに対して、スロット情報も表示されます。たとえば、*eth1 [A6] Intel Corporation 82576 Gigabit Network Connection* などと表示されます。ここで、スロット情報は角括弧で囲まれ、*A6* は、スロットＡの 6番目のポートを指します。現在、最高 3種類のスロット(A、B、C)があり、各スロットに対して最高 8種類のポートがあります。オンボードタイプのインターフェースカードは、*[MGMT1]* および *[MGMT2]* と表示されます。

スロット情報は、WebAdminの次の場所で表示されます。

- *インタフェース& ルーティング> インタフェース> インタフェース*
- *インタフェース& ルーティング> インタフェース> ハードウェア*
- WebAdminにある、すべての*ハードウェア*ドロップダウンリスト、およびハードウェアインターフェース情報が表示されているリスト。

フレキシブルスロットが装備されているアプライアンスの種類の最新情報は、Sophos UTM Webサイトを参照してください。

6.1.1.3 グループ

2つ以上のインタフェースをグループにまとめることができます。グループ化により、設定タスクを簡素化することができます。マルチパスルールを作成する場合に、すべてのアップリンクインタフェースではなく、定義したアップリンクインタフェースグループでのみトラフィックの分散を行うには、グループを設定する必要があります。

*グループ*インタフェースを設定するには、次の手順に従います。

1. ***インターフェース*タブで、*新規 インタフェース*をクリックします。**
   *インターフェースの追加*ダイアログボックスが開きます。
2. **次の設定を行います。**
   名前：インタフェースを説明する名前を入力してください。

   タイプ：ドロップダウンリストから*グループ*を選択します。

   インタフェース：グループ化するインタフェースを追加します。

   コメント(オプション)：説明などの情報を追加します。
3. ***保存*をクリックします。**
   グループがインタフェースリストに追加されます。グループにはステータスがありません。

特定タイプのインタフェースのみ表示する場合は、ドロップダウンリストから表示するインタフェースのタイプを選択します。インタフェースを編集または削除するには、対応するボタンをクリックします。

6.1.1.4 3G/UMTS

Sophos UTM は、3G/UMTS USBスティックを使用したネットワーク接続をサポートしています。

3G/UMTSインタフェースを設定するには、次の手順に従います。

1. *インターフェース*タブで、*新規インタフェース*をクリックします。
   *インターフェースの追加*ダイアログボックスが開きます。

2. 次の設定を行います。
   名前：インタフェースを説明する名前を入力してください。

   タイプ：ドロップダウンリストから*3G/UMTS*を選択します。

   ハードウェア：ドロップダウンリストからUSBモデムスティックを選択します。USBスティックを差し込んだ後で、リブートする必要があります。

   ネットワーク：モバイルネットワークタイプを*GSM/W-CDMA*、*CDMA*、または*LTE*から選択します。

   IPv4/IPv6デフォルトGW（オプション）：プロバイダのデフォルトゲートウェイを使用する場合、このオプションを選択します。

   PIN（オプション）：PINが設定されている場合、SIMカードのPINを入力します。

   APN自動選択（オプション）：デフォルトで、使用するAPN（アクセスポイント名）はUSBモデムスティックから取得されます。チェックボックスのチェックを外す場合、*APN*フィールドにAPN情報を入力します。

   ユーザ名/パスワード（オプション）：必要な場合、モバイルネットワークのユーザ名とパスワードを入力します。

   ダイヤル文字列（オプション）：プロバイダが異なるダイヤル文字列を使用している場合、ここに入力します。デフォルトは`*99#`です。

   コメント（オプション）：説明などの情報を追加します。

3. 次の詳細設定を任意で行います。
   初期化文字列：USBモデムスティックを初期化するための文字列を入力します。USBモデムスティックに応じて初期化文字列の調整が必要になる可能性があります。この場合、初期化文字列は当該USBモデムスティックのマニュアルで確認できます。必要なマニュアルがない場合、デフォルト設定の*ATZ*を維持してください。

   リセット文字列：USBモデムスティックのリセット文字列を入力します。USBモデムスティックに応じてリセット文字列の調整が必要になる可能性があります。この場合、リセット文字列は当該USBモデムスティックのマニュアルで確認できます。必要なマニュアルがない場合、デフォルト設定の*ATZ*を維持してください。

   MTU：インタフェースの最大伝送単位をバイト単位で入力します。トラフィックマネジメントを使用する場合は、インタフェースタイプに対応する値をここに入力する必要があります。イ

ンタフェースタイプに対して妥当な値がデフォルトで入力されています。この設定の変更は、技術的に熟練したユーザのみが行ってください。ここに不正な値を入力すると、インタフェースが使用不可能になる場合があります。1500バイトを超えるMTUサイズは、通信事業者とネットワークカードでサポートされていることが必要です(例:ギガビットインタフェース)。デフォルトで、*3G/UMTS*インタフェースタイプには1500バイトのMTUが設定されています。

デフォルトのルートメトリック:インタフェースのデフォルトのルートメトリックを入力します。メトリック値は同じ宛先へのルートを区別して優先するために使用され、すべてのインタフェースで有効です。

非対称(オプション):接続のアップリンクとダウンリンクの帯域幅が同一でない場合に、ダッシュボードにこれを反映させたいときは、このオプションを選択します。選択すると、2つのテキストボックスが表示されます。ここに最大アップリンク帯域幅をMbpsまたはKbps単位で入力します。ドロップダウンリストから適切なユニットを選択します。

表示する最大(オプション):ダッシュボードに反映させたい場合は、ここに接続の最大ダウンリンク帯域幅を入力できます。帯域幅はMbpsまたはKbps単位で入力できます。ドロップダウンリストから適切なユニットを選択します。

4. ***保存*をクリックします。**
システムが設定の有効性を確認します。チェックに成功すると、新しいインタフェースがインタフェースリストに表示されます。インタフェースはまだ有効ではありません(トグルスイッチはグレー表示)。

5. **インタフェースを有効にします。**
インタフェースを有効にするには、トグルスイッチをクリックします。

これでインタフェースが有効になります(トグルスイッチは緑色)。インタフェースがまだ*無効*と表示される場合があります。システムが構成を行い、設定をロードするまで、しばらく時間がかかります。*有効*が表示されたら、インタフェースは完全に動作可能です。

特定タイプのインタフェースのみ表示する場合は、ドロップダウンリストから表示するインタフェースのタイプを選択します。インタフェースを編集または削除するには、対応するボタンをクリックします。

6.1.1.5 イーサネット

内部または外部ネットワークにスタティックイーサネット接続するためのネットワークカードを設定するには、NIC及びIPアドレスとネットマスクを設定する必要があります。

スタティックイーサネットインタフェースを設定するには、次の手順に従ってください。

1. ***インターフェース*タブで、*新規 インタフェース*をクリックします。**
   *インターフェースの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前 : インタフェースを説明する名前を入力してください。

   タイプ: ドロップダウンリストから*イーサネット*を選択します。

   ハードウェア: ドロップダウンリストからインタフェースを選択します。

   > ヒント – インターネットなどの外部接続には、SysIDがeth1のネットワードカードを選択してください。1枚のネットワークカードを、*イーサネット*インタフェースおよび*PPP over Ethernet* *PPPoE DSL* 接続または*PPTP over Ethernet* *PPPoA DSL* 接続として同時に使用することはできません。

   動的**IP**動的IPアドレスを使用する場合に有効化します。

   IPv4/IPv6アドレス: インタフェースのIPアドレスを入力します。

   ネットマスク: ネットマスク(IPv4)を選択するか、IPv6ネットマスクを入力します。

   IPv4/IPv6デフォルト**G/W**(オプション): スタティックに定義されたデフォルトゲートウェイを使用する場合、このオプションを選択します。

   デフォルト**G/W**(オプション): デフォルトゲートウェイのIPアドレスを入力します。

   > 注 – IPv4 および IPv6 アドレスを同時に使用するよう、インタフェースを設定することができます。

   コメント(オプション): 説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**
   ホスト名 : ISPがシステムのホスト名の受信を要求する場合、ここに入力します。

   MTU: インタフェースの最大伝送単位をバイト単位で入力します。トラフィックマネジメントを使用する場合は、インタフェースタイプに対応する値をここに入力する必要があります。インタフェースタイプに対して妥当な値がデフォルトで入力されています。この設定の変更は、技術的に熟練したユーザのみが行ってください。ここに不正な値を入力すると、インタフェースが使用不可能になる場合があります。1500バイトを超えるMTUサイズは、通信事業者とネットワークカードでサポートされていることが必要です(例: ギガビットインタフェース)。デフォルトで、*イーサネット*インタフェースタイプには1500バイトのMTUが設定されています。

デフォルトのルートメトリック: インタフェースのデフォルトのルートメトリックを入力します。メトリック値は同じ宛先へのルートを区別して優先するために使用され、すべてのインタフェースで有効です。

プロキシ**ARP**: 機能を有効にするには、チェックボックスにチェックを入れます。デフォルトでは、*プロキシARP*機能は無効(オフ)になっています。このオプションはブロードキャストタイプのインタフェースで使用できます。これを選択すると、がそのインタフェース上のトラUTMフィックをその「背後にある」ホストの代わりに対して「引きつけ」、受け渡します。直接接続されたインタフェースルートがあるすべてのホストに対してこの処理が行われます。これにより、ファイアウォールを実行したまま、「透過的な」ネットワークブリッジを構築することができます。この機能の他の利用方法としては、ISPのルータが「公式」ネットワークのみをイーサネットインタフェースに受け入れる場合があります(ホストルートを使用しない)。

非対称(オプション):接続のアップリンクとダウンリンクの帯域幅が同一でない場合に、ダッシュボードにこれを反映させたいときは、このオプションを選択します。選択すると、2つのテキストボックスが表示されます。ここに最大アップリンク帯域幅をMbpsまたはKbps単位で入力します。ドロップダウンリストから適切なユニットを選択します。

表示する最大(オプション):ダッシュボードに反映させたい場合は、ここに接続の最大ダウンリンク帯域幅を入力できます。帯域幅はMbpsまたはKbps単位で入力できます。ドロップダウンリストから適切なユニットを選択します。

4. ***保存*をクリックします。**
   システムが設定の有効性を確認します。チェックに成功すると、新しいインタフェースがインタフェースリストに表示されます。インタフェースはまだ有効ではありません(トグルスイッチはグレー表示)。

5. **インタフェースを有効にします。**
   インタフェースを有効にするには、トグルスイッチをクリックします。

   これでインタフェースが有効になります(トグルスイッチは緑色)。インタフェースがまだ*無効*と表示される場合があります。システムが構成を行い、設定をロードするまで、しばらく時間がかかります。*有効*が表示されたら、インタフェースは完全に動作可能です。

特定タイプのインタフェースのみ表示する場合は、ドロップダウンリストから表示するインタフェースのタイプを選択します。インタフェースを編集または削除するには、対応するボタンをクリックします。

6.1.1.6 イーサネットVLAN

UTMを仮想LANに接続するためには、タグ付け可能なドライバのあるネットワークカードが必要になります。タグとは、イーサネットヘッダの一部としてパケットに付けられる2バイトのヘッダです。タグには、パケットの送信先となるVLANの番号が格納されます。VLANの番号は12ビット数で、最大4095の仮想LANまで許可します。WebAdminでは、この数を*VLANタグ*と呼びます。

注 – は、Sophosタグ付け可能なネットワークインタフェースカードのリストを管理しています。*ハードウェア互換性リスト HCL* はSophos Knowledgebaseから利用可能です。「HCL」を検索用語として使用して、該当するページを探してください。

イーサネットVLANインタフェースを設定するには、次の手順に従ってください。

1. ***インターフェース*タブで、*新規インタフェース*をクリックします。**
   *インターフェースの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:インタフェースを説明する名前を入力してください。

   タイプ:ドロップダウンリストから*イーサネットVLAN Ethernet VLAN* を選択します。

   ハードウェア:ドロップダウンリストからインタフェースを選択します。

   動的IP:動的IPアドレスを使用する場合、このオプションを選択します。

   VLANタグ:このインタフェースに対して使用するVLANタグを入力します。

   IPv4/IPv6アドレス:インタフェースのIPアドレスを入力します。

   ネットマスク:ネットマスク(IPv4)を選択するか、IPv6ネットマスクを入力します。

   IPv4/IPv6デフォルト**G/W**(オプション):スタティックに定義されたデフォルトゲートウェイを使用する場合、このオプションを選択します。

   デフォルト**G/W**(オプション):デフォルトゲートウェイのIPアドレスを入力します。

   注 –IPv4およびIPv6アドレスを同時に使用するよう、インタフェースを設定することができます。

   コメント(オプション):説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**

MTU: インタフェースの最大伝送単位をバイト単位で入力します。トラフィックマネジメントを使用する場合は、インタフェースタイプに対応する値をここに入力する必要があります。インタフェースタイプに対して妥当な値がデフォルトで入力されています。この設定の変更は、技術的に熟練したユーザのみが行ってください。ここに不正な値を入力すると、インタフェースが使用不可能になる場合があります。1500バイトを超えるMTUサイズは、通信事業者とネットワークカードでサポートされていることが必要です(例:ギガビットインタフェース)。デフォルトで、*イーサネットVLAN*インタフェースタイプには1500バイトのMTUが設定されています。

デフォルトのルートメトリック: インタフェースのデフォルトのルートメトリックを入力します。メトリック値は同じ宛先へのルートを区別して優先するために使用され、すべてのインタフェースで有効です。

プロキシ**ARP**: 機能を有効にするには、チェックボックスにチェックを入れます。デフォルトでは、*プロキシARP*機能は無効(オフ)になっています。このオプションはブロードキャストタイプのインタフェースで使用できます。これを選択すると、がそのインタフェース上のトラUTMフィックをその「背後にある」ホストの代わりに対して「引きつけ」、受け渡します。直接接続されたインタフェースルートがあるすべてのホストに対してこの処理が行われます。これにより、ファイアウォールを実行したまま、「透過的な」ネットワークブリッジを構築することができます。この機能の他の利用方法としては、ISPのルータが「公式」ネットワークのみをイーサネットインタフェースに受け入れる場合があります(ホストルートを使用しない)。

非対称(オプション):接続のアップリンクとダウンリンクの帯域幅が同一でない場合に、ダッシュボードにこれを反映させたいときは、このオプションを選択します。選択すると、2つのテキストボックスが表示されます。ここに最大アップリンク帯域幅をMbpsまたはKbps単位で入力します。ドロップダウンリストから適切なユニットを選択します。

表示する最大(オプション):ダッシュボードに反映させたい場合は、ここに接続の最大ダウンリンク帯域幅を入力できます。帯域幅はMbpsまたはKbps単位で入力できます。ドロップダウンリストから適切なユニットを選択します。

4. ***保存*をクリックします。**
   システムが設定の有効性を確認します。チェックに成功すると、新しいインタフェースがインタフェースリストに表示されます。インタフェースはまだ有効ではありません(トグルスイッチはグレー表示)。

5. **インタフェースを有効にします。**
   インタフェースを有効にするには、トグルスイッチをクリックします。

これでインタフェースが有効になります（トグルスイッチは緑色）。インタフェースがまだ*無効*と表示される場合があります。システムが構成を行い、設定をロードするまで、しばらく時間がかかります。*有効*が表示されたら、インタフェースは完全に動作可能です。

特定タイプのインタフェースのみ表示する場合は、ドロップダウンリストから表示するインタフェースのタイプを選択します。インタフェースを編集または削除するには、対応するボタンをクリックします。

6.1.1.7 DSL (PPPoE)

設定には、ご利用のISPが提供したユーザ名とパスワードを含むDSL接続情報が必要になります。VDSLもこのインタフェースタイプでサポートされています。

注 – DSL 接続を有効にすると、UTMはご利用の ISP に1日 24時間接続されます。したがって、ご利用の ISP の請求が接続時間ベースではなく定額制または帯域幅ベースの料金システムであることをご確認ください。

DSL（PPPoE）インタフェースを設定するには、次の手順に従ってください。

1. ***インターフェース*タブで、*新規インタフェース*をクリックします。**
   *インターフェースの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前：インタフェースを説明する名前を入力してください。

   タイプ：ドロップダウンリストから*DSL PPPoE*を選択します。

   ハードウェア：ドロップダウンリストからインタフェースを選択します。

   VDSL：このチェックボックスは、ご利用の接続がVDSL接続である場合のみ選択します。*MTU*は`1476`に変更されます。

   スタティック**PPPoE IP**（オプション）：ISPに割り当てられたスタティックIPアドレスがある場合、チェックボックスにチェックを入れ、表示されるテキストボックスにIPアドレスと該当するネットマスクを入力します。

   - **IPv4**アドレス：インタフェースのIPアドレスを入力します。
   - ネットマスク：ドロップダウンリストからネットマスクを選択するか、IPv6ネットマスクを入力します（あるいはその両方）。

注 – インタフェースを設定して、IPv4およびIPv6アドレスを同時に使用することができます。

IPv4/IPv6デフォルト**GW**（オプション）：プロバイダのデフォルトゲートウェイを使用する場合、このオプションを選択します。

ユーザ名：ISPから入手したユーザ名を入力します。

パスワード：ISPから入手したパスワードを入力します。

コメント（オプション）：説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**
 MTU：インタフェースの最大伝送単位をバイト単位で入力します。トラフィックマネジメントを使用する場合は、インタフェースタイプに対応する値をここに入力する必要があります。インタフェースタイプに対して妥当な値がデフォルトで入力されています。この設定の変更は、技術的に熟練したユーザのみが行ってください。ここに不正な値を入力すると、インタフェースが使用不可能になる場合があります。1500バイトを超えるMTUサイズは、通信事業者とネットワークカードでサポートされていることが必要です（例：ギガビットインタフェース）。デフォルトで、*DSL (PPPoE)*インタフェースタイプには 1492 バイトの MTU が設定されています。

 デフォルトのルートメトリック：インタフェースのデフォルトのルートメトリックを入力します。メトリック値は同じ宛先へのルートを区別して優先するために使用され、すべてのインタフェースで有効です。

 VLANタグ（*VDSL*が有効な場合のみ）：PPPoEパケットに追加するVLANタグを入力します。正しいタグについては、VDSL プロバイダに問い合わせてください。デフォルトでは7であり、現在はDeutsche TelekomのPPPoE接続用に使用されています。

 日次再接続：接続を終了および再開する時間を定義します。*無し*を選択するか、具体的な時間を指定することができます。

 再接続ディレイ：ここで、再接続ディレイを変更できます。デフォルトでは、*5秒*に設定されています。ご利用の ISP がこれより長い遅延を要求している場合は、*1分*や*15分*に設定できます。

 非対称（オプション）：接続のアップリンクとダウンリンクの帯域幅が同一でない場合に、ダッシュボードにこれを反映させたいときは、このオプションを選択します。選択すると、2つ

のテキストボックスが表示されます。ここに最大アップリンク帯域幅をMbpsまたはKbps単位で入力します。ドロップダウンリストから適切なユニットを選択します。

表示する最大（オプション）：ダッシュボードに反映させたい場合は、ここに接続の最大ダウンリンク帯域幅を入力できます。帯域幅はMbpsまたはKbps単位で入力できます。ドロップダウンリストから適切なユニットを選択します。

マルチリンク：有効にすると、複数の PPP 接続を 1つにまとめることができます。マルチリンク PPP 接続が機能できるのは、使用しているISP がマルチリンクンPPPをサポートしている場合だけです。

マルチリンクスレーブ：上記で選択したハードウェアをマルチリンクにバンドルしたいインターフェースを選択します。

4. *保存*をクリックします。
   システムが設定の有効性を確認します。チェックに成功すると、新しいインタフェースがインタフェースリストに表示されます。インタフェースはまだ有効ではありません（トグルスイッチはグレー表示）。

5. **インタフェースを有効にします。**
   インタフェースを有効にするには、トグルスイッチをクリックします。

   これでインタフェースが有効になります（トグルスイッチは緑色）。インタフェースがまだ*無効*と表示される場合があります。システムが構成を行い、設定をロードするまで、しばらく時間がかかります。*有効*が表示されたら、インタフェースは完全に動作可能です。

特定タイプのインタフェースのみ表示する場合は、ドロップダウンリストから表示するインタフェースのタイプを選択します。インタフェースを編集または削除するには、対応するボタンをクリックします。

6.1.1.8 DSL (PPPoA/PPTP)

PPPoA（*PPP over ATM Protocolプ*ロトコル）した接続を設定するには、UTM上の未使用のイーサネットインタフェースと、イーサネットポート付きの外部 ADSL モデムが必要です。インターネットへの接続は2つの個別の接続で行ないます。UTMとADSLモデム間では、*PPTP over Ethernet プロトコル*を使用して接続を確立します。ADSLモデムは、*PPP over ATM Dialingプロトコル*を使用してISPに接続します。

設定には、ご利用のインターネットサービスプロバイダ（ISP）が提供したユーザ名とパスワードを含むDSL接続情報が必要になります。

注 – DSL 接続を有効にすると、UTMはご利用の ISP に1日 24時間接続されます。したがって、ご利用の ISP の請求が接続時間ベースではなく定額制または帯域幅ベースの料金システムであることをご確認ください。

DSL（PPPoA/PPTP）インタフェースを設定するには、次の手順に従ってください。

1. *インターフェース*タブで、*新規 インタフェース*をクリックします。
   *インターフェースの追加*ダイアログボックスが開きます。
2. **次の設定を行います。**
   名前 : インタフェースを説明する名前を入力してください。

   タイプ: ドロップダウンリストから*DSL PPPoA/PPTP* を選択します。

   ハードウェア: ドロップダウンリストからインタフェースを選択します。

   IPv4/IPv6デフォルト**GW**（オプション）: プロバイダのデフォルトゲートウェイを使用する場合、このオプションを選択します。

   ユーザ名 : ISPから入手したユーザ名を入力します。

   パスワード: ISPから入手したパスワードを入力します。

   コメント(オプション) : 説明などの情報を追加します。
3. **次の詳細設定を任意で行います。**
   モデム**IP**: お使いのADSLモデムのIPアドレスをここに入力します。このアドレスは通常、ISPから、あるいはモデムハードウェアとともに提供されるので、変更できません。
   例 : `10.0.0.138`（AonSpeed）。

   NICアドレス: モデムに接続されているUTM上のネットワークカードのIPアドレスをここに入力します。このアドレスはモデムと同じサブネット内にある必要があります。
   例 : `10.0.0.140`（AonSpeed）。

   NICネットマスク: 使用するネットワークマスクをここに入力します。例 : `255.255.255.0`（AonSpeed）。

   pingアドレス（オプション）: ICMP ping要求に応答するインターネット上のホストのIPアドレスを入力します。UTMと外部ネットワーク間の接続をテストするには、PPTPリンクの反対側ホストのIPアドレスを入力する必要があります。ご利用のISPのDNSサーバを使用することができます。UTMがこのホストにping要求を送信します。応答がない場合は、接続不良です。

MTU：インタフェースの最大伝送単位をバイト単位で入力します。トラフィックマネジメントを使用する場合は、インタフェースタイプに対応する値をここに入力する必要があります。インタフェースタイプに対して妥当な値がデフォルトで入力されています。この設定の変更は、技術的に熟練したユーザのみが行ってください。ここに不正な値を入力すると、インタフェースが使用不可能になる場合があります。1500バイトを超えるMTUサイズは、通信事業者とネットワークカードでサポートされていることが必要です（例：ギガビットインタフェース）。デフォルトでは、1492バイトのMTUが*DSL PPPoA* インタフェースタイプに設定されています。

デフォルトのルートメトリック：インタフェースのデフォルトのルートメトリックを入力します。メトリック値は同じ宛先へのルートを区別して優先するために使用され、すべてのインタフェースで有効です。

日次再接続：接続を終了および再開する時間を定義します。*無し*を選択するか、具体的な時間を指定することができます。

再接続*ディレイ*：ここで、再接続ディレイを変更できます。デフォルトでは、*5秒*に設定されています。ご利用の ISP がこれより長い遅延を要求している場合は、*1分*や*15分*に設定できます。

非対称（オプション）：接続のアップリンクとダウンリンクの帯域幅が同一でない場合に、ダッシュボードにこれを反映させたいときは、このオプションを選択します。選択すると、2つのテキストボックスが表示されます。ここに最大アップリンク帯域幅をMbpsまたはKbps単位で入力します。ドロップダウンリストから適切なユニットを選択します。

表示する最大（オプション）：ダッシュボードに反映させたい場合は、ここに接続の最大ダウンリンク帯域幅を入力できます。帯域幅はMbpsまたはKbps単位で入力できます。ドロップダウンリストから適切なユニットを選択します。

4. ***保存*をクリックします。**
   システムが設定の有効性を確認します。チェックに成功すると、新しいインタフェースがインタフェースリストに表示されます。インタフェースはまだ有効ではありません（トグルスイッチはグレー表示）。

5. **インタフェースを有効にします。**
   インタフェースを有効にするには、トグルスイッチをクリックします。

   これでインタフェースが有効になります（トグルスイッチは緑色）。インタフェースがまだ*無効*と表示される場合があります。システムが構成を行い、設定をロードするまで、しばらく時間がかかります。*有効*が表示されたら、インタフェースは完全に動作可能です。

特定タイプのインタフェースのみ表示する場合は、ドロップダウンリストから表示するインタフェースのタイプを選択します。インタフェースを編集または削除するには、対応するボタンをクリックします。

6.1.1.9 モデム PPP

設定には、UTMにシリアルインタフェースと外部PPPモデムが必要になります。また、ユーザ名とパスワードを含むDSLアクセスデータも必要です。これらのデータは、インターネットサービスプロバイダ(ISP)から入手できます。

モデム PPP インタフェースを設定するには、次の手順に従ってください。

1. ***インターフェース*タブで、*新規インタフェース*をクリックします。**
   *インターフェースの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:インタフェースを説明する名前を入力してください。

   タイプ:ドロップダウンリストから *モデム PPP* を選択します。

   ハードウェア:ドロップダウンリストからインタフェースを選択します。

   IPv4/IPv6デフォルト**GW**(オプション):プロバイダのデフォルトゲートウェイを使用する場合、このオプションを選択します。

   ユーザ名:ISPから入手したユーザ名を入力します。

   パスワード:ISPから入手したパスワードを入力します。

   ダイヤル文字列:電話番号を入力します。例:`5551230`

   コメント(オプション):説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**
   回線速度:UTMとモデムの間の接続に対して、速度をbps単位で設定します。一般的な値は57,600 bpsと115,200 bpsです。

   フローコントロール:データフローをコントロールする方法を選択します。

   データがシリアル接続経由で転送される場合、システムで受信データを十分に速く処理できない可能性があります。データの損失が発生しないようにするためには、データフローのコントロール方法が必要になります。シリアル接続では、次の2つの方法を使用できます。

   - *ハードウェア*信号
   - *ソフトウェア*信号

PPP接続では、すべての8ビットがデータ転送回線に使用され、転送されるデータにはコマンドサイン*Control S*と*Control Q*のバイトが含まれるため、デフォルト設定の*ハードウェア*を維持し、シリアル接続ケーブルを使用することをお勧めします。

初期化文字列：モデムを初期化するための文字列を入力します。モデムに応じて初期化文字列の調整が必要になる可能性があります。この場合、初期化文字列は該当モデムのマニュアルで確認できます。必要なマニュアルがない場合、デフォルト設定の*ATZ*を維持してください。

リセット文字列：モデムのリセット文字列を入力します。モデムに応じてリセット文字列の調整が必要になる可能性があります。この場合、リセット文字列は該当モデムのマニュアルで確認できます。必要なマニュアルがない場合、デフォルト設定の*ATZ*を維持してください。

MTU：インタフェースの最大伝送単位をバイト単位で入力します。トラフィックマネジメントを使用する場合は、インタフェースタイプに対応する値をここに入力する必要があります。インタフェースタイプに対して妥当な値がデフォルトで入力されています。この設定の変更は、技術的に熟練したユーザのみが行ってください。ここに不正な値を入力すると、インタフェースが使用不可能になる場合があります。1500バイトを超えるMTUサイズは、通信事業者とネットワークカードでサポートされていることが必要です（例：ギガビットインタフェース）。デフォルトで、*モデム PPP* インタフェースタイプには1492バイトのMTUが設定されています。

デフォルトのルートメトリック：インタフェースのデフォルトのルートメトリックを入力します。メトリック値は同じ宛先へのルートを区別して優先するために使用され、すべてのインタフェースで有効です。

非対称（オプション）：接続のアップリンクとダウンリンクの帯域幅が同一でない場合に、ダッシュボードにこれを反映させたいときは、このオプションを選択します。選択すると、2つのテキストボックスが表示されます。ここに最大アップリンク帯域幅をMbpsまたはKbps単位で入力します。ドロップダウンリストから適切なユニットを選択します。

表示する最大（オプション）：ダッシュボードに反映させたい場合は、ここに接続の最大ダウンリンク帯域幅を入力できます。帯域幅はMbpsまたはKbps単位で入力できます。ドロップダウンリストから適切なユニットを選択します。

4. ***保存*をクリックします。**
   システムが設定の有効性を確認します。チェックに成功すると、新しいインタフェースがインタフェースリストに表示されます。インタフェースはまだ有効ではありません（トグルスイッチはグレー表示）。

5. **インタフェースを有効にします。**

インタフェースを有効にするには、トグルスイッチをクリックします。

これでインタフェースが有効になります(トグルスイッチは緑色)。インタフェースがまだ*無効*と表示される場合があります。システムが構成を行い、設定をロードするまで、しばらく時間がかかります。*有効*が表示されたら、インタフェースは完全に動作可能です。

特定タイプのインタフェースのみ表示する場合は、ドロップダウンリストから表示するインタフェースのタイプを選択します。インタフェースを編集または削除するには、対応するボタンをクリックします。

6.1.2 追加アドレス

1つのネットワークカードで追加IPアドレス(別名*エイリアス*)を*設定できます*。この機能を使用すると、1つの物理ネットワークカード上で複数の論理ネットワークを管理することができます。また、これを使用して、NAT(ネットワークアドレス変換)を実行しているUTMにさらなるアドレスを割り当てることもできます。

標準イーサネットインタフェースで追加アドレスを設定するには、次の手順に従ってください。

1. ***追加アドレス*タブで、*新規追加アドレス*をクリックします。**
   *追加アドレスを追加*ダイアログが開きます。

2. **次の設定を行います。**
   名前:新しい追加アドレスを説明する名前を入力してください。

   インタフェース:アドレスを割り当てるインタフェースをドロップダウンリストから選択します。

   IPv4/IPv6アドレス:インタフェースの追加IPアドレスを入力します。

   ネットマスク:ドロップダウンリストからネットマスクを選択するか、IPv6ネットマスクを入力します(あるいはその両方)。

   > 注 – IPv4およびIPv6アドレスを同時に使用するよう、インタフェースを設定することができます。

   コメント(オプション):説明などの情報を追加します。

3. ***保存*をクリックします。**
   システムが設定の有効性を確認します。チェックに成功すると、新しいインタフェースがインタフェースリストに表示されます。インタフェースはまだ有効ではありません(トグルスイッチはグレー表示)。

4. **追加アドレスを有効にします。**

追加アドレスを有効にするには、トグルスイッチをクリックします。

これで追加アドレスが有効になります(トグルスイッチは緑)。追加アドレスはまだ*ダウン*と表示されている場合があります。システムが構成を行い、設定をロードするまで、しばらく時間がかかります。*アップ*というメッセージが表示されると、追加アドレスは完全に機能するようになっています。

追加アドレスを編集または削除するには、対応するボタンをクリックします。

6.1.3 リンクアグリゲーション

リンクアグリゲーションは、「ポートトランキング」または「NICボンディング」とも呼ばれ、これによって複数のイーサネットネットワークポートを1つの仮想インタフェースに集約することができます。集約されたポートはシステム上で1つのIPアドレスとして表示されます。リンクアグリゲーションは、どの単体 NIC よりも リンク速度を向上させたり、いずれかのポートまたはスイッチで障害が発生した場合に冗長性を維持して基本フェイルオーバーおよびフォールトトレランス機能を提供したりするために役に立ちます。障害が発生したポートやスイッチにルーティングされているすべてのトラフィックは自動的にリルートされ、残りのポートまたはスイッチのいずれかを使用するようになります。このフェイルオーバーは、接続を使用しているシステムに対して完全に透過的です。

注 – HA環境では、イーサネット接続を別のHAユニット上にすることもできます。

リンクアグリゲーショングループは最大4つまで定義することができます。グループには1つまたは複数のインタフェースを含めることができます。

リンクアグリゲーショングループ(LAG)を作成するには、次の手順に従います。

1. **各LAGに対して、追加するインタフェースを選択します。**
   グループは、設定されているインタフェースまたは1つ以上の設定されていないインタフェース(あるいはその両方)で構成することができます。

   設定されているインタフェースを使用するには、*変換インタフェース*ドロップダウンリストからインタフェースを選択します。設定されていないインタフェースを使用するには、それぞれのチェックボックスにチェックを入れます。

2. **LAGを有効にします。**
   *このグループを有効化*ボタンをクリックして、グループを有効にします。

   リンクアグリゲーショングループを設定すると、*インタフェース*タブでインタフェース定義を作成するときに、新しいLAGインタフェース(`lag0`など)を選択できるようになります。ボンディングインタフェースの上部で、次のいずれかを作成できます。

- イーサネットスタティック
- イーサネットVLAN
- イーサネットDHCP
- エイリアスインタフェース

LAGを無効にするには、LAGを構成するインタフェースのチェックボックスのチェックを外して、*このグループを更新*をクリックし、警告メッセージを確認します。LAGインタフェースのステータスが、*サポート* > *詳細* > *インタフェーステーブル*タブに表示されます。

6.1.4 アップリンクバランス

アップリンクバランス機能を使用すると、複数のインターネットアップリンクを組み合わせて、バックアップ用アップリンクを使用可能にするか、複数のアップリンクに負荷を分散することができます。組み合わせることができるアップリンクは最大32です。ベーシックガードサブスクリプションでは、2つのアップリンクだけが組み合わせされていることに注意してください。

デフォルトゲートウェイを備えた既存インタフェースに加えて、デフォルトゲートウェイをインタフェースに割り当てると、アップリンクバランスが自動的に有効になります。デフォルトゲートウェイを装備するすべてのインタフェースは、*アクティブインタフェース*ボックスに追加され、以降はアップリンクバランスにより、これらのインタフェースの間で自動的にバランシングが行われます。デフォルトゲートウェイを装備する他のインタフェースもすべて自動的に追加されます。

*マルチパスルール*タブでは、トラフィックのバランシングを行うための特定のルールを定義できます。

アップリンクバランスを手動でセットアップするには、次の手順に従います。

1. **アップリンクバランスを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、*アップリンクバランス*エリアが編集可能になります。

2. **アクティブインタフェースを選択します。**
   フォルダアイコンをクリックしてインタフェースを1つ以上追加し、オブジェクトリストからインタフェースをドラッグします。複数のインタフェースの場合、クライアントからのトラフィックは送信元によってバランシングされます。つまり、1つの送信元から送られたすべてのトラフィックが同じインタフェースを使用する一方で、別の送信元からのトラフィックは別のインタフェースに送信できます。いずれかのインタフェースを使用できない場合、トラフィックは残りのインタフェースによってテイクオーバーされます。

> **注 –** 最初にアップリンクバランスが自動的に有効化された段階で、*アクティブインタフェース*リストには既にデフォルトゲートウェイを装備するすべてのインタフェースが表示されます。リストからインタフェースを削除すると、インタフェースの*デフォルトゲートウェイ*チェックボックスから自動的にチェックが外れます。したがって、デフォルトゲートウェイを装備するすべてのインタフェースは、このリストに示されるか、その下の*スタンバイインタフェース*ボックスに示されるかのいずれかになります。しかし、デフォルトゲートウェイを装備しないインタフェースを追加して、後にデフォルトゲートウェイのアドレスを入力することができます。

> **注 –** インタフェースの順序は重要な意味を持ちます。1つのインタフェースだけが使用できる構成で、UTM自体によって送信されるパケットでは、デフォルトで、最初に使用できるインタフェースが使用されます。インタフェースの順序は、ボックスでソートアイコンをクリックして変更できます。

ボックスのヘッダでスケジューラの編集アイコンを使用すると、個々のバランシング動作およびアクティブインタフェースのインタフェースパーシスタンスを設定することができます。

加重：加重とは、あるインタフェースが処理するトラフィック量を他のインタフェースに対して相対的に示すもので、0～100の間で設定できます。加重ラウンドロビンアルゴリズムが使用され、値が大きいほど、該当インタフェースにルーティングされるトラフィックが多くなります。相対的な値であるため、合計して100にする必要はありません。たとえば、インタフェース1の値を100に、インタフェース2の値を50に、インタフェース3の値を0に設定することなどができます。この場合、インタフェース2のトラフィック量はインタフェース1の半分となり、インタフェース3は他のインタフェースが使用可能でない場合にのみ使用されます。0の値は、より値が大きい他のインタフェースが常に使用されることを示します（他のインタフェースが使用可能であれば）。

パーシステンス：インタフェースパーシスタンスとは、特定の属性を持つトラフィックが常に同じアップリンクインタフェース経由でルーティングされるようにする技術です。パーシスタンスのデフォルトのタイムアウト時間は1時間です。

3. **スタンバイインタフェースの選択** *オプション*
ここでは、すべてのアクティブインタフェースが使用不能になった場合にのみ使用されるフェイルオーバーインタフェースをオプションで追加することができます。この場合、与えられた順序で最初に使用できるスタンバイインタフェースが使用されます。インタフェースの順序は、ボックスでソートアイコンをクリックして変更できます。

4. **モニタリングの設定の変更** *オプション*

デフォルトでは、インタフェース障害の可能性を検出するために*自動 モニタリング*が有効になっています。つまり、すべてのアップリンク バランシング インタフェースからインターネット上の特定のホストに 15秒間隔で接続することにより、それらのインタフェースの状態(健全性)がモニタリングされます。デフォルトでは、ホストのモニタリングは、1つのルート DNS サーバーまでのルート上にある、ping を許可する 3番目のホップです。なお、ユーザーはサーバープールをモニタリングするためのホストを自分で定義することができます。これらのホストには、ping 以外の別のサービスを選択し、モニタリング間隔とタイムアウトを変更できます。

モニタリングホストが応答を送信しなくなった場合、そのインタフェースは機能していない(デッド(dead)である)と見なされるため、それ以降配信に使用されません。ダッシュボードでは、インタフェースの *リンク*列に*エラー*と表示されます。

注 – 同じモニタリング設定が、アップリンクモニタリング(*アップリンクモニタリング* > *詳細*)とアップリンクバランス(*インターフェース* > *アップリンクバランス*)に対して使用されます。

5. *適用***をクリックします。**
   設定が保存されます。

   トグルスイッチが緑色に変わります。

*アップリンクインタフェース*という名前の新しい仮想ネットワークインタフェースが自動的に作成され、Sophos UTMの他の機能(IPsecルールなど)で使用できるようになっています。仮想ネットワークインタフェース *アップリンクインタフェース*は、インタフェースリストに追加されたすべてのアップリンクインタフェースから構成されています。

さらに、*アップリンクプライマリアドレス*という名前の新しいネットワークグループが自動的に作成され、のSophos UTM他の機能(ファイアウォールルールなど)で使用できるようになっています。これは、すべての *アップリンクインタフェース*のプライマリアドレスを参照します。

DynDNSが使用されている場合や、リモートサーバがすべてのアップリンクインタフェースのIPアドレスを受け付けることができる場合は、インタフェースで障害が発生したときに、次に使用可能なインタフェースを介してオープンなVPNトンネルを自動的に再確立することができます。前提条件としては、IPsecルールが *ローカル インタフェース*として *アップリンクインタフェース*を使用する必要があります。

モニタリング ホストの定義

サーバプールをモニタリングするためのホストを自分で定義するには、次の手順に従います。

1. *自動モニタリング*チェックボックスのチェックを外します。
   *モニタリングホスト*ボックスが編集可能になります。

2. **モニタリングホストを追加します。**
   任意のホストを使用する代わりに、モニタリングに使用するホストを1つ以上選択または追加します。複数のホストでインタフェースをモニタリングする場合、定義された時間内にすべてのモニタリングホストが応答しない場合にのみ、インタフェースがデッドとみなされます。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

   > 注 – 選択したホストがインタフェースに関連付けられている場合は、このインタフェースのモニタリングのみに使用されます。ホストがインタフェースに関連付けられていない場合は、すべてのインタフェースのモニタリングに使用されます。選択したホストによりカバーされていないインタフェースは、自動モニタリングによりモニタリングされます。

   ボックスのヘッダにあるモニタリング設定アイコンをクリックして、モニタリングの詳細を設定します:

   モニタリングタイプ: モニターチェックのサービスプロトコルを選択します。モニタリング用に*TCP*(TCP接続の確立)、*UDP*(UDP接続の確立)、*Ping*(ICMP Ping)、*HTTPホスト HTTP Host* (HTTP要求)、または*HTTPSホスト HTTPS Hosts* (HTTPS要求)のいずれかを選択します。*UDP*を使用する場合、ping要求が最初に送信され、成功した場合は、続いてペイロード0のUDP パケットが送信されます。pingが成功しなかった場合や、ICMPポートに到達できない場合、この接続はダウンしているとみなされます。

   ポート(*TCP*および*UDP*のモニタリングタイプのみ): 要求の送信先のポート番号。

   URL(オプション、*HTTP/Sホスト*のモニタリングタイプのみ): 要求するURL。URLにポート情報を追加することで、デフォルトポートの80または443以外のポートを使用することもできます。例、`http://example.domain:8080/index.html`。URLを指定しない場合は、ルートディレクトリが要求されます。

   間隔: ホストをチェックする間隔を秒単位で入力します。

   タイムアウト: モニタリングホストが応答を送信する最大時間を秒単位で入力します。インタフェースのすべてのモニタリングホストがこの時間内に応答しない場合、インタフェースがデッドとみなされます。

3. *適用*をクリックします。
   設定が保存されます。

6.1.5 マルチパスルール

インタフェース& ルーティング > *インタフェース* > *マルチパスルール*タブでは、アップリンクバランス用のルールを設定できます。ルールは、トラフィックのバランシングを行うべき複数のインタフェースがある場合に、*アップリンクバランス*タブでアクティブインタフェースに適用されます。マルチパスルールがない場合は、すべてのサービスは送信元によってバランシングされます。つまり、1つの送信元から送られたすべてのトラフィックが同じインタフェースを使用する一方で、別の送信元からのトラフィックは別のインタフェースに送信できます。マルチパスルールによって、このデフォルトのインタフェースパーシスタンスを変更することができます。

注 – マルチパスルールは、サービスタイプTCP、UDP、IPに対してセットアップできます。

マルチパスルールを作成するには、次の手順に従います。

1. ***マルチパスルール*タブで、*新規 マルチパスルール*をクリックします。**
   *マルチパスルールの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前 : マルチパスルールを説明する名前を入力してください。

   位置 : ルールの優先順位を定義する位置番号。番号が小さいほど優先順位が高くなります。ルールは昇順に照合されます。あるルールが一致すると、それ以降、それより大きい番号のルールは評価されません。より具体的なルールをリストの上部に配置して、曖昧なルールが最後に照合されるようにします。

   送信元 : 照合する送信元IPアドレスまたはネットワークを選択または追加します。

   サービス: 照合するネットワークサービスを選択または追加します。

   宛先 : 照合する宛先IPアドレスまたはネットワークを選択または追加します。

   ヒント – 定義を追加する方法は、*定義 とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

   I/F パーシステンス: *インタフェースパーシスタンス*とは、特定の属性を持つトラフィックが常に同じアップリンクインタフェース経由でルーティングされるようにする技術です。パーシスタンスのデフォルトのタイムアウト時間は1時間ですが、このタイムアウトは *アップリンクバランス*タブで変更できます。を基準にパーシスタンスを定めるかを定義することができます。

- コネクション別：（デフォルト）バランシングはコネクションに基づいて行われます。つまり、特定のコネクションに属するすべてのトラフィックが同じインタフェースを使用する一方で、別のコネクションのトラフィックは別のインタフェースに送信できます。
- 送信元別：バランシングは送信元IPアドレスに基づいて行われます。つまり、1つの送信元から送られたすべてのトラフィックが同じインタフェースを使用する一方で、別の送信元からのトラフィックは別のインタフェースに送信できます。

> 注 – プロキシを使用している場合、送信元に基づくパーシスタンスは実行できません。これは、オリジナルの送信元情報が維持されないことによります。HTTPプロキシによるトラフィックは、オリジナルのクライアント送信元IPアドレスに一致するため、インターフェース パーシスタンス ルール*送信元別*に準拠します。

- 宛先別：バランシングは宛先IPアドレスに基づいて行われます。つまり、1つの宛先に送られるすべてのトラフィックが同じインタフェースを使用する一方で、別の宛先へのトラフィックは別のインタフェースに送信できます。
- 送信元/宛先別：バランシングは送信元/宛先IPアドレスの組み合わせに基づいて行われます。つまり、送信元Aから宛先Bに送られるすべてのトラフィックが同じインタフェースを使用します。別の組み合わせのトラフィックは別のインタフェースに送信できます。また、上記の注にも注意してください。
- インタフェース別：*バインドインタフェース*ドロップダウンリストからインタフェースを選択します。ルールに該当するすべてのトラフィックは、このインタフェース経由でルーティングされます。インタフェースで障害が発生し、後続のルールが一致しない場合、接続はデフォルトの動作にフォールバックします。

コメント（オプション）：説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**
   分散先（インタフェースによるパーシスタンス以外）：フィールドにインタフェースグループを追加します。ルールに該当するすべてのトラフィックは、このグループのインタフェースでバランシングされます。デフォルトでは、*アップリンクインタフェース*が選択されるため、すべてのアップリンクインタフェースで接続がバランシングされます。

   インタフェースのエラーがあればルールをスキップ（*Itf. パーシスタンス*が *インタフェース別*に設定されている場合のみ利用可能）：選択すると、インタフェースで障害が発生したときに、次のマルチパスルールをトラフィックで使用します。選択していない場合は、インタフェースの障害が発生しても、他のマルチパスルールは定義されたトラフィックで使用されません。たとえば、無効な送信者のIPアドレスであるという理由で受信者がメールをスパムメールに

分類してしまうことを防ぐために、SMTPトラフィックを確実に特定のスタティックIPアドレスだけに送信するように設定したい場合にはこういう設定が適切です。

4. ***保存*をクリックします。**
新しいマルチパスルールが *マルチパスルール*リストに追加されます。

マルチパスルールを有効にします。

5. 新しいルールはデフォルトで無効になっています(トグルスイッチはグレー表示)。ルールを有効にするには、トグルスイッチをクリックします。これでルールが有効になります(トグルスイッチは緑色)。

ルールを編集 または削除 するには、対応 するボタンをクリックします。

6.1.6 ハードウェア

インタフェース& ルーティング > *インタフェース* > *ハードウェア*タブには、設定されているすべてのインタフェースが、イーサネットオペレーションモード、MACアドレスなどの情報と共に表示されます。UTM ハードウェアデバイスで、各インタフェースに対し、オートネゴシエーションを有効または無効にすることができます。

オートネゴシエーション: 通常、2つのネットワークデバイス間のイーサネット操作モード(1000BASE-T 全二重、100BASE-T 全二重、100BASE-T 半二重、10BASE-T 全二重、10BASE-T 半二重など)が自動的にネゴシエートされ、両方のデバイスでサポートされる最適な操作モードが選択されます。このとき、速度は高速(1000Mbps など)が低速(100Mbps など)より優先され、同じ速度では全二重の方が半二重より優先されます。

警告 – 1000 Mbpsのオペレーションを適切に機能させるためには、IEEE標準802.3abにより義務付けられているように、常にオートネゴシエーションが必要になります。このため、*リンクモード* *1000BASE-T*のインタフェースの *オートネゴシエーション*を決してオフにしないようにしてください。ネットワークリンクにタイミング障害が発生して、サービスが低下したり、障害が発生する可能性があります。100 Mbpsおよび10 Mbpsオペレーションでは、オートネゴシエーションがオプションですが、できる限り使用することを推奨します。

オートネゴシエーションはデフォルトで有効化されています。まれなケースでオートネゴシエーションをオフにする必要がある場合、対応するインタフェースカードの *編集*ボタンをクリックして、表示される*NIC パラメータの編集*ダイアログボックスの *リンクモード*ドロップダウンリストで設定を変更します。ドロップダウンリストはUTMハードウェアデバイスでのみ使用可能である点に注意が必要です。*保存*をクリックして変更を保存します。

警告 – オートネゴシエーションを無効にするときは注意してください。これにより、不一致が生じ、パフォーマンスが大幅に低下したり、接続が切断したりする可能性もあります。該当するネットワークインタフェースカードがWebAdminへのインタフェースである場合、WebAdminへのアクセスが切断されてしまいます。

オートネゴシエーションや速度の変更の結果、インタフェースのネットワークリンクが失われた場合には、設定を元に戻すことでインタフェースを通常のオペレーションに戻すことができます。切断されているインタフェースでは、オートネゴシエーションや速度を確実に変更することができません。したがって、最初にオートネゴシエーションをオンにしてからUTMをリブートして通常のオペレーションに戻します。

HA *リンクモニタリング*: 冗長化が有効である場合、設定されたすべてのインタフェースでリンクステータスがモニタリングされます。リンクに障害が発生した場合、テイクオーバーが引き起こされます。設定されたインタフェースが常に接続されている訳ではない場合(管理インタフェースなど)、このインタフェースのHAリンクモニタリングは無効にしてください。無効にしないと、すべてのHAリンクのステータスが「未接続(UNLINKED)」のままになります。HA リンクモニタリングを無効にするには、各インタフェースカードの*編集*ボタンをクリックして、表示される*NIC パラメータの編集*ダイアログウィンドウで設定を変更します。*保存*をクリックして変更を保存します。

仮想**MAC**の設定: デバイスのMACアドレスを変更できると便利な場合があります。たとえば、ISPによっては、モデムに接続されているデバイスに変更があった場合にこのモデムをリセットし、デバイスのMACアドレスをリセットする必要があります。MACアドレスを前のデバイスの値に設定することで、モデムのリセットを回避することができます。

は、UTMデバイスのオリジナルの MAC アドレスを上書きするのではなく、仮想 MAC アドレスを設定します。これを行うには、該当するインタフェースカードの*編集*ボタンをクリックします。表示される*NIC パラメータの編集*ダイアログウィンドウで、*仮想 MAC の設定*チェックボックスにチェックを入れ、有効な MAC アドレスを入力します。*保存*をクリックして変更を保存します。

オリジナルの MAC アドレスに復元するには、該当するインタフェースカードの*編集*ボタンをクリックします。表示される*NIC パラメータの編集*ダイアログウィンドウで、*仮想 MAC の設定*チェックボックスのチェックを外します。*保存*をクリックして変更を保存します。

6.2 サービス品質 QoS

一般的に、*サービス品質*(QoS)とは、選択されたネットワークトラフィックにより良いサービスを提供する制御メカニズムを示し、特に、保証された帯域幅という点で優先することを意味します。Sophos UTMでは、優先トラフィックは、*QoS*タブで設定します。この設定では、ネットワークの 2点

間を通過する特定タイプの送信ネットワークトラフィックに対し、保証された帯域幅を確保できますが、一方で、受信トラフィックのシェーピングは SFQ（*確率的不偏キューイング*）あるいは RED（*ランダム初期検知*）などのさまざまなテクニックによって内部的に最適化されます。

6.2.1 ステータス

QoS > *ステータス*タブには、QoSを設定できるインタフェースがリストされます。デフォルトでは、QoSは各インタフェースに対して無効になっています。

インタフェースに対してQoSを設定するには、次の手順に従います。

1. **各インターフェースの*編集*ボタンをクリックします。**
   *インターフェースの編集*ダイアログボックスが開きます。

2. **次の設定を行います。**
   *ダウンリンク***kbit/秒** / *アップリンク***kbit/秒**：ISPによって提供されるアップリンクとダウンリンクの帯域幅（Kbps）を入力します。たとえば、アップリンクとダウンリンクの両方に5Mビット/秒（Mbps）のインターネット接続を設定するには、`5120`と入力します。

   帯域幅が変動する場合は、ISPが保証した最低の値を入力します。たとえば、アップリンクとダウンリンクの両方に0.8Mビット/秒（Mbps）の変動のある5Mビット/秒（Mbps）のインターネット接続を使用する場合は、4300Kビット/秒（Kbps）と入力します。利用できる帯域幅が一時的に設定した最低保証値より高くなると、ゲートウェイは新しい帯域幅を考慮して予想して、優先トラフィックの帯域幅のパーセンテージが同様に高くなるようにしますが、これは残念ながら、その反対には作用しません。

   アップリンクを制限：このオプションを選択すると、QoS機能は、設定されたダウンリンクとアップリンクの帯域幅を、このインタフェースを通過するトラフィックを優先順位付けするための計算ベースとして使用します。デフォルトでは*アップリンクを制限*オプションは選択されており、以下のインタフェースタイプに使用されます。

   - イーサネットスタティックインタフェース（ゲートウェイとインターネット間にルータが配備され、ルータが提供する帯域幅がわかっているもの）
   - 標準VLANインタフェース（ゲートウェイとインターネット間にルータが配備され、ルータが提供する帯域幅がわかっているもの）
   - DSL（PPPoE）
   - DSL（PPPoA）
   - モデム（PPP）

トラフィックシェーピングの計算ベースがインタフェースの最大速度で決定されるインタフェースの *アップリンクを制限* チェックボックスからチェックを外します。ただし、これは以下のインタフェースタイプにのみ適用されます。

- イーサネットスタティックインタフェース（インターネットに直接接続）
- イーサネットVLANインタフェース（インターネットに直接接続）
- イーサネットDHCP

特定のアップリンク制限が指定されていないインタフェースでは、QoS機能が全トラフィックを均等にシェーピングします。たとえば、イーサネットDHCPインタフェース上のVoIPトラフィックに512Kビット/秒（Kbps）を設定した場合に、利用できる帯域幅が半分になったときは、256Kビット/秒がこのトラフィックに使用されます（比例シェーピングは、固定最大制限に依存するインタフェースと対照的に、双方向に機能することに注意してください）。

ダウンロードイコライザ：有効にすると、*確率的不偏キューイング*（SFQ）および *ランダム初期検知*（RED）キューアルゴリズムがネットワークの輻輳を回避します。設定したダウンリンク速度に達すると、ストリームを使用するほとんどのダウンリンクのパケットはドロップします。

アップロードオプティマイザ：有効にすると、送信TCP接続の確立（*SYN*フラグが設定されたTCPパケット）、TCP接続のACK（確認応答）パケット（*ACK*フラグが設定され、パケット長が40～60バイトのTCPパケット）、およびDNSルックアップ（ポート53上のUDPパケット）が自動的に優先されます。

3. ***保存*をクリックします。**
   設定が保存されます。

4. **インターフェースに対してQoSを有効にします。**
   インタフェースのトグルスイッチをクリックします。

   トグルスイッチが緑色に変わります。

6.2.2 トラフィックセレクタ

トラフィックセレクタは、QoSが扱う特定タイプのネットワークトラフィックを記述したQoSの定義と見なすことができます。これらの定義は、後で帯域幅プール定義の中で使用されます。帯域幅プール定義では、帯域幅全体の制限や特定量の最低帯域幅の保証など、QoSによるこのトラフィックの取り扱い方法について定義できます。

トラフィックセレクタを作成するには、以下の手順に従います。

1. **_トラフィックセレクタ_タブで、_新規 トラフィックセレクタ_をクリックします。**
   _トラフィックセレクタの追加_ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:このトラフィックセレクタを説明する名前を入力します。

   セレクタタイプ:以下のタイプを定義できます。

   - トラフィックセレクタ:トラフィックセレクタを使用すると、トラフィックは1つのサービスまたはサービスグループに基づいてシェーピングされます。
   - アプリケーションセレクタ:アプリケーションセレクタを使用すると、トラフィックはアプリケーションに基づいてシェーピングされます。つまり、使用するポートやサービスを問わず、どのトラフィックがどのアプリケーションに属しているかに基づきます。
   - グループ:複数のサービスおよびアプリケーションセレクタを1つのトラフィックセレクタルールにまとめることができます。グループを定義するには、単体のセレクタをいくつか定義している必要があります。

   送信元:QoSを有効にする送信元ネットワークを追加または選択します。

   サービス: _トラフィックセレクタ_のみ。QoSを有効にするネットワークサービスを追加または選択します。事前に定義したさまざまなサービスやサービスグループから選択できます。たとえば、固定帯域幅をVoIP接続に予約する場合は、VoIPプロトコル(SIPおよびH.323)を選択します。

   宛先:QoSを有効にする宛先ネットワークを追加または選択します。

   ヒント – 定義を追加する方法は、_定義とユーザ_ > _ネットワーク定義_ > _ネットワーク定義_ページで説明しています。

   制御基準: _アプリケーションセレクタ_のみ。アプリケーションタイプに基づいてトラフィックをシェーピングするか、分類に基づくダイナミックフィルタによってコントロールするかを選択します。

   - アプリケーション:トラフィックは、アプリケーションに基づいてシェーピングされます。_制御するアプリケーション_ボックスでアプリケーションを1つ以上選択します。
   - ダイナミックフィルタ:トラフィックは、カテゴリに基づいてシェーピングされます。_制御するカテゴリ_ボックスで分類を1つ以上選択します。

制御するアプリケーション/カテゴリ: *アプリケーションセレクタ*のみ。フォルダアイコンをクリックして、アプリケーション/カテゴリを選択します。ダイアログウィンドウが開きます。これについては、次のセクションで詳しく説明します。

生産性:*ダイナミックフィルタ*のみ。選択した生産性スコアが反映されます。

リスク: *ダイナミックフィルタ*のみ。選択したリスクスコアが反映されます。

注 – 一部のアプリケーションはシェーピングできません。これは、Sophos UTMの適切なオペレーションのために必要です。このようなアプリケーションは、*アプリケーション選択*ダイアログウィンドウのアプリケーションテーブルでチェックボックスがオフになっています。たとえば、*WebAdmin*、*Teredo*、*SixXs*(IPv6トラフィック用)、*Portal*(ユーザーポータルのトラフィック用)などが該当します。ダイナミックフィルタを使用すると、これらのアプリケーションのシェーピングも自動的に制限されます。

コメント(オプション):説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**
TOS/DSCP(*トラフィックセレクタ*のセレクタタイプのみ):特殊なケースでは、送信元、宛先、およびサービスだけでなく、IPヘッダのTOSまたはDSCP フラグによって、QoSが処理するトラフィックを区別することが有益になります。

- *オフ*: このデフォルトオプションでは、上で選択した送信元、サービス、および宛先と一致するすべてのトラフィックがQoSにより処理されます。
- **TOS** ビット: QoSが処理するトラフィックを特定のTOS(サービスタイプ)ビット設定のIPパケットに制限する場合は、このオプションを選択します。以下の設定から選択できます。
  - 通常サービス
  - 金額的コストの最小化
  - 信頼性の最大化
  - スループットの最大化
  - 遅延の最小化
- **DSCP** ビット: QoSが処理するトラフィックを特定のDSCP(差別化サービスコードポイント)ビット設定のIPパケットに制限する場合は、このオプションを選択します。単一の*DSCP 値*(0~63 の整数)を指定するか、または*DSCP クラス*リストから事前に定義した値を選択できます(*BE default dscp (000000)*など)。

送受信データ量: 接続によってそれまでに送信されたバイト量に基づいてトラフィックセレクタを一致させる場合は、このチェックボックスにチェックを入れます。この機能を使用すると、通常のHTTPトラフィックを制限することなく、大規模なHTTPアップロードの帯域幅を制限することなどができます。

- 送受信: 特定のトラフィック量を超過する接続のみのトラフィックセレクタを定義する場合は、ドロップダウンリストから*次の値より大*を選択します。特定の量を下回る接続のトラフィックセレクタを定義する場合は、*次の値より小*を選択します。

- キロバイト:トラフィック量のしきい値を入力します。

ヘルパ: 一部のサービスは、データ転送で動的ポート範囲を使用します。それぞれの接続について、使用するポートは制御チャネル経由でエンドポイント間でネゴシエートされます。UTMは、特別なコネクショントラッキングヘルパを使用して、制御チャネルをモニタリングし、どの動的ポートが現在使用されているかを判断します。動的ポート経由で送信されたトラフィックをトラフィックセレクタに含める場合は、上部の*サービス*ボックスで*任意*を選択し、*ヘルパー*ドロップダウンリストから適切なサービスを選択します。

4. ***保存*をクリックします。**
新しいセレクタが*トラフィックセレクタ*リストに表示されます。

多くのトラフィックセレクタを定義した場合は、1つのトラフィックセレクタグループに複数のセレクタをまとめることで、より便利に使用することが可能になります。

このトラフィックセレクタまたはトラフィックセレクタグループは、それぞれの帯域幅プールで使用できます。これらのプールは*帯域幅プール*タブで定義できます。

アプリケーションまたはカテゴリの選択ダイアログウィンドウ

アプリケーションコントロールルールを作成する際は、*管理するアプリケーション(カテゴリ)を1つ以上選択してください*というダイアログウィンドウからアプリケーションまたはアプリケーションカテゴリを選択する必要があります。

ダイアログウィンドウの下部に表示されるテーブルには、選択可能なアプリケーションまたは定義したカテゴリに属するアプリケーションが表示されます。デフォルトでは、すべてのアプリケーションが表示されます。

ダイアログウィンドウの上部には、テーブルに表示されるアプリケーション数を制限するための3つの設定オプションがあります。

- *カテゴリ*: アプリケーションはカテゴリ別にグループ分けされています。このリストには、利用可能なすべてのカテゴリが表示されます。デフォルトでは、すべてのカテゴリが選択されています。つまり、下部に表示されるテーブルには、利用可能なすべてのアプリケーションが

表示されます。表示されるアプリケーションを特定のカテゴリに絞り込むには、クリックしてカテゴリリストを開き、1つ以上のカテゴリを選択します。

- 生産性:アプリケーションは、生産性への影響(つまり生産性にこのアプリケーションが与える影響の度合い)によっても分類されています。例:一般的なビジネスソフトウェアのSalesforceのスコアは5です。つまり、これを使用することで生産性が向上します。一方、オンラインゲームのFarmvilleのスコアは1で、これを使用すると生産性が低下します。ネットワークサービスDNSのスコアは3で、生産性への影響は中立的です。

- リスク:アプリケーションは、使用時のリスク(マルウェア、ウイルス感染、攻撃)によっても分類されています。数値が高いほど、リスクも高くなります。

ヒント – それぞれのアプリケーションには情報アイコンがあり、クリックすると各アプリケーションの説明が表示されます。テーブルヘッダのフィルタフィールドを使用して、テーブル内を検索することができます。

次に、*新規トラフィックセレクタの作成*ダイアログボックスで選択したコントロールのタイプに応じて、以下を行います。

- ダイナミックフィルタでコントロールする場合:*カテゴリ*ボックスでカテゴリを選択し、*適用*をクリックして、選択したカテゴリをルールに適用します。

- アプリケーションでコントロールする場合:テーブルで、アプリケーションの前のチェックボックスをクリックし、コントロール対象のアプリケーションを選択します。*適用*をクリックして、選択したアプリケーションをルールに適用します。

*適用*をクリックするとダイアログウィンドウが閉じ、トラフィックセレクタルールの設定の編集を続けることができます。

6.2.3 帯域幅プール

*QoS > 帯域幅プール*タブで、帯域幅を管理するための帯域幅プールを定義して管理できます。帯域幅プールでは、特定の送信トラフィックタイプに対して保証された帯域幅を確保し、オプションで、最大帯域幅制限によって制限します。

帯域幅プールを作成するには、以下の手順に従います。

1. ***帯域幅プール*タブで、インタフェースを選択します。**
   *インタフェースに関連付け*ドロップダウンリストから、帯域幅プールを作成するインタフェースを選択します。

2. ***新規帯域幅プール*をクリックします。**

*帯域幅プールの追加*ダイアログボックスが開きます。

3. **次の設定を行います。**
   名前:この帯域幅プールを説明する名前を入力します。

   位置:位置番号。これによって帯域幅プールの優先順位が定義されます。番号が小さいほど優先順位が高くなります。帯域幅プールは昇順に照合されます。ある帯域幅プールが一致すると、それ以降、それより大きい番号の帯域幅プールは評価されません。より具体的な帯域幅プールをリストの上部に配置して、曖昧な帯域幅プールが最後に照合されるようにします。たとえば、一般的なWebトラフィック(HTTP)と特定ホストへのWebトラフィックにトラフィックセレクタを設定した場合は、帯域幅プールリストの最上部に後者のトラフィックセレクタを使用する帯域幅プールを配置します(つまり、位置1をそれに選択します)。

   帯域幅:この帯域幅プール用に予約するアップリンク帯域幅をKビット単位で入力します。たとえば、特定タイプのトラフィックに1Mビット/秒(Mbps)を予約する場合は、`1024`と入力します。

   > 注 – 帯域幅プールに割り当てられるのは、利用可能な全帯域幅の90%までです。ゲートウェイは常に帯域幅の10%をいわゆるシェーピングされていないトラフィック用に予約します。上記の例で言えば、アップリンクのインターネット接続が5Mビット/秒(Mbps)で、VoIPトラフィックにできるだけ多くの帯域幅を割り当てたい場合は、最大4608Kビット/秒(Kbps)を入力できます。

   帯域幅の上限を指定:上記の*帯域幅*フィールドに入力した値は、特定の種類のトラフィック用に予約される保証された帯域幅を示します。しかし、帯域幅プールは通常、可能であれば、そのトラフィック用により多くの帯域幅を割り当てます。特定のトラフィックが一定量以上の帯域幅を使用しないようにしたい場合は、このオプションを選択して、この帯域幅プールによって使用される帯域幅の割り当てを上限値に制限します。

   トラフィックセレクタ:この帯域幅プールに使用するトラフィックセレクタを選択します。

   コメント(オプション):説明などの情報を追加します。

4. ***保存*をクリックします。**
   新しい帯域幅プールが*帯域幅プール*リストに表示されます。

   ルールを有効にします。

5. 新しいルールはデフォルトで無効になっています(トグルスイッチはグレー表示)。ルールを有効にするには、トグルスイッチをクリックします。これでルールが有効になります(トグルスイッチは緑色)。

帯域幅プールを編集または削除するには、対応するボタンをクリックします。

6.2.4 ダウンロード帯域幅調整

*QoS > ダウンロード帯域幅調整*タブで、受信トラフィックの帯域幅を調整するルールを定義して管理できます。設定したしきい値より速くパケットが送信される場合、過剰なパケットはファイアウォールルールのログファイルにリストされることなく、ただちにドロップされます。TCP輻輳回避メカニズムの結果として、影響を受ける送信者は、ドロップされたパケットに応じて送信率を下げる必要があります。

ダウンロード帯域幅調整ルールを作成するには、次の手順に従います。

1. ***ダウンロード帯域幅調整*タブで、インタフェースを選択します。**
   *インタフェースに関連付け*ドロップダウンリストから、ダウンロード帯域幅調整を作成するインタフェースを選択します。

2. ***新規ダウンロード帯域幅調整ルール*をクリックします。**
   *帯域幅調整ルールの追加*ダイアログボックスが開きます。

3. **次の設定を行います。**
   名前：このダウンロード帯域幅調整ルールを説明する名前を入力してください。

   優先順位：ルールの優先順位を定義する位置番号。番号が小さいほど優先順位が高くなります。ルールは昇順に照合されます。あるルールが一致すると、それ以降、それより大きい番号のルールは評価されません。より具体的な帯域幅ルールをリストの上部に配置して、曖昧な帯域幅ルールが最後に照合されるようにします。

   限度 **kbit/s** ：特定のトラフィックの上限（単位はKbit）です。,たとえば、特定タイプのトラフィックで1Mビット/秒（Mbps）を予約する場合は、1024と入力します。

   制限：上で指定した制限を適用するべきトラフィックの送信元および宛先の組み合わせ。

   - 共有：制限は、既存のすべての接続に渡って等しく分配されます。つまり、このルールによって指定されたトラフィックの総合ダウンロード速度は、特定の値に制限されます。
   - *それぞれの送信元アドレス*：制限は、それぞれの特定の送信元アドレスに適用されます。
   - *それぞれの宛先アドレス*：制限は、それぞれの特定の宛先アドレスに適用されます。
   - *それぞれの送信元/宛先*：制限は、それぞれの特定のペアの送信元アドレスおよび宛先アドレスに適用されます。

トラフィックセレクタ: ダウンロード速度を調整したいトラフィックセレクタを選択します。選択したトラフィックセレクタの間で、指定した制限が配分されます。

コメント(オプション):説明などの情報を追加します。

4. *保存*をクリックします。
新しいダウンロード帯域幅調整ルールが*ダウンロード帯域幅調整*リストに表示されます。

ルールを有効にします。

5. 新しいルールはデフォルトで無効になっています(トグルスイッチはグレー表示)。ルールを有効にするには、トグルスイッチをクリックします。これでルールが有効になります(トグルスイッチは緑色)。

ルールを編集または削除するには、対応するボタンをクリックします。

6.2.5 詳細

カプセル化の後も分類を維持する

カプセル化後にパケットが他のトラフィックセレクタが一致しない場合に、元のサービスのトラフィックセレクタと引き続き一致することを確認する場合は、このチェックボックスにチェックを入れます。

トラフィックセレクタへのカプセル化されたIP パケットの割り当ては、次のように機能します。

1. 元のIPパケットを与えられた順序で既存のトラフィックセレクタと比較します。パケットが最初に一致するトラフィックセレクタに割り当てられます(内部 -> HTTP -> 任意など)。

2. IPパケットがカプセル化され、サービスが変更されます(IPsecなどへ)。

3. カプセル化したパケットを与えられた順序で既存のトラフィックセレクタと比較します。パケットが最初に一致するトラフィックセレクタに割り当てられます(内部 -> IPsec -> 任意など)。

4. 一致するトラフィックセレクタがない場合の割り当ては、*カプセル化後もクラシフィケーションを保持*オプションに依存します。

    - このオプションが選択されている場合、カプセル化したパケットが手順1で検出したトラフィックセレクタに割り当てられます。

    - このオプションが選択されていない場合、カプセル化したパケットはトラフィックセレクタに割り当てられないため、帯域幅プールの一部にすることができません。

明示的な輻輳通知 ECN サポート

ECN(明示的な輻輳通知)とはインターネットプロトコルの拡張であり、ネットワーク輻輳のエンドツーエンドな通知をパケットのドロップなしで許可します。ECNは、接続の両エンドポイントの間で使用のネゴシエートが成功している場合にのみ機能します。このチェックボックスにチェックを入れ

ると、UTMは、ECN使用の意向を伝える情報を送信します。他のエンドポイントが合意すると、エンドポイントがECN情報を交換します。下位のネットワークと関与するルータもECNをサポートしている必要があります。

6.3 アップリンクモニタリング

*インタフェース& ルーティング > アップリンクモニタリング*メニューでは、アップリンク接続をモニタリング(監視)し、接続ステータスが変化したときに自動的に適用するアクションを定義することができます。

たとえば、別のリンクを使用してバックアップVPNトンネルを自動的にオンにしたり、エイリアスIPアドレスを無効にしてモニタリングサービスをトリガすることができます。

6.3.1 グローバル

*アップリンクモニタリング > グローバル*タブで、アップリンクのモニタリングを有効または無効にできます。

アップリンクモニタリングを有効にするには、トグルスイッチをクリックします。

トグルスイッチが緑色に変わります。

アップリンクのモニタリングが有効であれば、*アップリンクステータス*セクションに、すべての現在のアップリンクインタフェースとその状態が表示されます:

- *オンライン:* アップリンク接続が確立され、機能しています。
- *オフライン:* モニタリングによれば、アップリンク接続が不良である。
- *ダウン:* アップリンクインタフェースが管理上無効であるか、ダイナミックインタフェースであれば、リモート PPPまたはDHCP サーバが動作していない。
- *スタンバイ:* インタフェースは、*インタフェース > アップリンクバランス*タブでスタンバイインタフェースとして定義され、現在は使用されていない。

注 – アップリンクバランスが有効であれば、アップリンクモニタリングが無効であっても、アップリンクは常にモニターされます。したがって、アップリンクモニタリングが無効であっても、アップリンクバランスが有効であれば、このページにアップリンクインタフェースが表示されます。この場合、モニタリング設定を*インタフェース > アップリンクバランス*タブで変更できます。

6.3.2 アクション

*インタフェース & ルーティング > アップリンクモニタリング > アクション*タブで、アップリンクの接続ステータスが変更になった場合に自動的に適用するアクションを定義できます。たとえば、アップリンク接続がダウンした場合は追加アドレスを無効にすることができます。

新しいアクションを作成するには、以下の手順に従います。

1. ***アクション*タブで、*新規アクション*をクリックします。**
   *アップリンクオフライン時の新規アクションの作成*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:アクションを説明する名前を入力します。

   タイプ:アクションを定義する接続タイプを選択します。

   - **IPsec** トンネル:IPsecトンネルに対するアクションを定義する場合は、ドロップダウンリストからこのオプションを選択します。
   - 追加アドレス:追加アドレスに対するアクションを定義する場合は、ドロップダウンリストからこのオプションを選択します。

   IPsec トンネル:(*IPsec トンネル*タイプにのみ利用可)IPsecトンネルを定義している場合は、ここでそれらのいずれかを選択できます。IPsecトンネルに関する詳細は、*リモートアクセス* > *IPsec*の章を参照してください。

   追加 アドレス:(*追加アドレス*タイプでのみ利用可能)追加アドレスを定義する場合、ここでいずれかのオプションを選択します。追加アドレスに関する詳細は、*インタフェース & ルーティング* > *インタフェース* > *追加アドレス*の章を参照してください。

   アクション:ここで*有効*または*無効*のいずれかを選択できます。つまり、アップリンクが中断した場合は、上記で選択したIPsecトンネルや追加アドレスが有効または無効になるように設定します。

   コメント(オプション):説明などの情報を追加します。

3. ***保存*をクリックします。**
   アクションは保存され、アップリンクの接続が中断すると適用されます。

アクションを編集または削除するには、対応するボタンをクリックします。

6.3.3 詳細

アップリンクモニタリング > *詳細*タブで、アップリンク接続の自動モニタリングを無効にしたり、モニタリング（監視）に使用する1つ以上のホストを定義できます。

デフォルトでは、インタフェース障害の可能性を検出するために*自動 モニタリング*が有効になっています。つまり、すべてのアップリンク バランシング インタフェースからインターネット上の特定のホストに 15秒間隔で接続することにより、それらのインタフェースの状態（健全性）がモニタリングされます。デフォルトでは、ホストのモニタリングは、1つのルート DNS サーバーまでのルート上にある、ping を許可する 3番目のホップです。なお、ユーザーはサーバープールをモニタリングするためのホストを自分で定義することができます。これらのホストには、ping 以外の別のサービスを選択し、モニタリング間隔とタイムアウトを変更できます。

各モニタリングホストには、一定期間接続を試み、いずれにも到達できない場合は、アップリンク接続はダウンしていると判断されます。その後、*アクション*タブで定義したアクションが実行されます。

> 注 – 同じモニタリング設定が、アップリンクモニタリング（*アップリンクモニタリング* > *詳細*）とアップリンクバランス（*インターフェース* > *アップリンクバランス*）に対して使用されます。

モニタリングにお客様のホストを使用するには、以下の手順に従います。

1. ***自動 モニタリング*チェックボックスのチェックを外します。**
   *モニタリングホスト*ボックスが編集可能になります。

2. **モニタリングホストを追加します。**
   任意のホストを使用する代わりに、モニタリングに使用するホストを1つ以上選択または追加します。複数のホストでインタフェースをモニタリングする場合、定義された時間内にすべてのモニタリングホストが応答しない場合にのみ、インタフェースがデッドとみなされます。定義を追加する方法は、*定義 とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

   > 注 – 選択したホストがインタフェースに関連付けられている場合は、このインタフェースのモニタリングのみに使用されます。ホストがインタフェースに関連付けられていない場合は、すべてのインタフェースのモニタリングに使用されます。選択したホストによりカバーされていないインタフェースは、自動モニタリングによりモニタリングされます。

ボックスのヘッダにあるモニタリング設定アイコンをクリックして、モニタリングの詳細を設定します:

モニタリングタイプ:モニターチェックのサービスプロトコルを選択します。モニタリング用に*TCP*(TCP接続の確立)、*UDP*(UDP接続の確立)、*Ping*(ICMP Ping)、*HTTPホスト HTTP Host* (HTTP要求)、または*HTTPSホスト HTTPS Hosts* (HTTPS要求)のいずれかを選択します。*UDP*を使用する場合、ping要求が最初に送信され、成功した場合は、続いてペイロード0のUDP パケットが送信されます。pingが成功しなかった場合や、ICMPポートに到達できない場合、この接続はダウンしているとみなされます。

ポート(*TCP*および*UDP*のモニタリングタイプのみ):要求の送信先のポート番号。

URL(オプション、*HTTP/Sホスト*のモニタリングタイプのみ):要求するURL。URLにポート情報を追加することで、デフォルトポートの80または443以外のポートを使用することもできます。例、`http://example.domain:8080/index.html`。URLを指定しない場合は、ルートディレクトリが要求されます。

間隔:ホストをチェックする間隔を秒単位で入力します。

タイムアウト:モニタリングホストが応答を送信する最大時間を秒単位で入力します。インタフェースのすべてのモニタリングホストがこの時間内に応答しない場合、インタフェースがデッドとみなされます。

3. ***適用*をクリックします。**
   設定が保存されます。

6.4 IPv6

Sophos UTMは、バージョン8より、IPv4の後継であるIPv6をサポートしています。

UTMの以下の機能は、IPv6を完全にまたは部分的にサポートします。

- WebAdminおよびユーザポータルへのアクセス
- SSH
- NTP
- SNMP
- SLAAC(ステートレスアドレス自動設定)およびDHCPv6クライアントはすべての動的インタフェースタイプをサポートしています。
- DNS

- DHCPサーバ
- BGP
- OSPF
- IPS
- ファイアウォール
- NAT
- ICMP
- サーバロードバランシング
- Webフィルタ
- アプリケーションコントロール
- WAF
- SMTP
- IPsec(サイト間のみ)
- Syslogサーバ

6.4.1 グローバル

*IPv6 > グローバル*タブでは、Sophos UTMのIPv6サポートを有効にすることができます。さらに、これを有効にすると、IPv6の情報(ステータス情報やプレフィックス委任情報など)がここに表示されます。

IPv6サポートはデフォルトでは無効になっています。IPv6を有効にするには、次の手順に従います。

1. ***グローバル*タブで、IPv6を有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチが緑色に変わります。以前にIPv6を有効化または設定したことがない場合は、*接続*エリアに*なし*と表示されます。

IPv6を有効にすると、複数のネットワークや、WebAdminでIPv6を明示的に参照しているその他のオブジェクト定義が表示されます。これらは、IPv4オブジェクトと同様に使用することができます。

注 – IPv6を有効にすると、ネットワークオブジェクトなどのアイコンに、該当オブジェクトがIPv6オブジェクトかIPv4オブジェクトか(あるいはその両方か)を示すマークが追加で表示されます。

6.4.2 プレフィックス広告

IPv6 > *プレフィックス広告*タブでは、Sophos UTMを設定して、クライアントにIPv6アドレスプレフィックスを割り当てて、クライアントが自力でIPv6アドレスを選択できるように設定することができます。プレフィックス広告(またはルータ通知)とは、IPv6の機能の1つであり、ルータ(この場合UTM)がIPv4におけるDHCPサーバと同じように機能します。ただし、ルータはクライアントにIPを直接割り当てません。代わりに、IPv6ネットワーク内のクライアントは、ルータとのプライマリ通信のためにいわゆるリンクローカルアドレスを自らに割り当てます。続いて、ルータがクライアントにネットワークセグメントのプレフィックスを伝えます。その後、クライアントはプレフィックスと自らのMACアドレスから成るIPアドレスを生成します。

新しいプレフィックスを作成するには、次の手順に従います。

1. ***プレフィックス広告*タブで、*新規プレフィックス*をクリックします。**
   *プレフィックスの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   インタフェース: 64ビットのネットマスクが設定されたIPv6アドレスを持つインタフェースを選択します。

   DNSサーバ1/2(オプション):DNSサーバのIPv6アドレス。

   ドメイン(オプション):クライアントに送信されるドメイン名を入力します(例:`intranet.example.com`)。

   有効期間:プレフィックスが有効となる期間。デフォルトは30日間です。

   推奨期間:この期間を超過すると、推奨されるライフタイムがまだ満了していない他のプレフィックスがクライアントに選択されます。デフォルトは7日間です。

3. **次の詳細設定を任意で行います。**
   ステートレス統合サーバ: このオプションはデフォルトで選択されています。プレフィックス広告を作成すると、DHCPv6サーバが自動的に起動されます。このDHCPv6設定は非表示であり、DHCP設定メニューでの表示や編集はできません。

   マネージド ステートフル :このオプションは、*ステートレス統合サーバ*が選択されている場合には利用できません。これにより、プレフィックス広告を有する同じインタフェース内で、ス

テートフルDHCPv6サーバを起動できます。DHCPv6サーバは、*ネットワークサービス> DHCP > サーバ*タブで設定できます。

その他の設定:このオプションは、*ステートレス統合サーバ*が選択されている場合には利用できません。これにより、所与のプレフィックスに対して所与のDNSサーバとドメイン名がDHCPv6経由で追加でアナウンスされます。現時点では、プレフィックス広告からDNS情報をフェッチできるクライアントは少ないため、この機能が役に立つます(RFC 5006/ RFC 6106)。

4. ***保存*をクリックします。**
   新しいプレフィックス設定が*プレフィックス広告*リストに表示されます。

6.4.3 再割り当て

*IPv6 > 再割り当て*タブで、プレフィックス変更の場合にIPv6 アドレスの自動再割り当てをUTMに管理させることができます。さらに、IPv6アドレスを手動で再割り当てすることができます。

以下のIPv6アドレスが変更されます:

- ホスト、ネットワーク、レンジの定義
- プライマリおよびセカンダリ インターフェース アドレス
- DHCPv6 サーバ範囲とマッピング
- DNS マッピング

トンネルブローカが提供するIPv6プレフィックスは再割り当てされません。

自動IPv6再割り当て

デフォルトでは、UTM によって管理されているIPv6 アドレスは、IPv6プレフィックス変更の際に自動再割り当てされます。プレフィックス変更は、DHCPv6プレフィックス委任によるISPで開始されます。再割り当てを無効にするには、チェックボックスのチェックを外し、*適用*をクリックします。

手動IPv6再割り当て

UTMによって管理されているIPv6アドレスを手動で再割り当てすることができます。これは、ISPを変更する場合に便利であり、新しいプロバイダは、DHCPv6で自動的に割り当てる代わりに、新しいIPv6プレフィックスをスタティックに割り当てることができます。

1. **再割り当てするIPv6アドレスの現在のプレフィックスを指定します。**
   *古いプレフィックス*フィールドにプレフィックスを入力します。

2. **新しいプレフィックスを指定します。**

*新しいプレフィックス*フィールドにプレフィックスを入力します。

3. ***適用*をクリックします。**
定義された現在のプレフィックスを持つIPv6アドレスが、すべて新しいプレフィックスで再割り当てされます。

6.4.4 6to4

*IPv6 > 6to4*タブでは、既存のIPv4ネットワーク上でIPv6アドレスを自動的にトンネリングするようにSophos UTMを設定することができます。6to4を使用すると、各IPv4アドレスに、マッピング先のIPv6ネットワークから`/48`プレフィックスが付加されます。生成されるIPv6アドレスは、プレフィックス`2002`と16進表記のIPv4アドレスから構成されます。

注 – *6to4*を有効にするか*トンネルブローカ*を使用するかのいずれかを選択できます。

特定のインタフェースのIPアドレストンネリングを有効にするには、次の手順に従います。

1. ***6to4*タブで6to4を有効化します。**
トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、*6to4*エリアと*詳細*エリアが編集可能になります。

2. **インタフェースを選択します。**
*インタフェース*ドロップダウンリストから、パブリックIPv6アドレスが設定されているインタフェースを選択します。

3. ***適用*をクリックします。**
設定が保存されます。

   トグルスイッチが緑色に変わり、インタフェースのステータスが*グローバル*タブに表示されます。

詳細

*サーバアドレス*を変更して、別の6to4リレーサーバを使用することができます。使用するには、*サーバアドレス*を入力し*適用*をクリックして、設定を保存します。

6.4.5 トンネルブローカー

*IPv6 > トンネルブローカー*タブでは、トンネルブローカの使用を有効にすることができます。トンネルブローカーは一部のISPが提供するサービスであり、これを利用するとIPv6アドレスを使用してイン

ターネットにアクセスできます。

注 – 6to4を有効にするか *トンネルブローカー*を使用するかのいずれかを選択できます。

Sophos UTMは、次のトンネルブローカーをサポートします。

- Teredo（匿名のみ）
- Freenet6（GoGo6）（匿名またはユーザアカウント使用）
- SixXS（ユーザアカウントが必要）
- Hurricane Electric（ユーザアカウントが必要）

トンネルブローカーを使用するには、次の手順に従います。

1. *トンネルブローカー***タブで、トンネルブローカの使用を有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチが緑色になり、*トンネルブローカー*エリアと*詳細*エリアが編集可能になります。Teredoの匿名認証を使用すると、トンネルブローカーはすぐに有効になります。接続ステータスが*グローバル*タブに表示されます。

SixXSトンネルを使用してIPv6接続が失われた場合、SixXSトンネルは自動的に再起動されません。この場合は、*ログとレポート* > *ログファイルの閲覧* > *今日のログファイル*に表示されているログファイルをチェックします。

トンネルブローカー

デフォルトのトンネルブローカー設定を変更できます。

認証：ドロップダウンリストから認証方法を選択します。

- **匿名**：この方法を使用すると、各ブローカにユーザアカウントを指定する必要はありません。割り当てられるIPアドレスは一時的なものです。
- **ユーザ**：各ブローカに登録して、ユーザアカウントを取得する必要があります。

ブローカ：ドロップダウンリストから他のブローカを選択できます。

ユーザ名（*ユーザ*のみで使用可能）：各ブローカにユーザ名を指定します。

パスワード（*ユーザ*のみで使用可能）：ユーザ名のパスワードを入力します。

設定を保存するには*適用*をクリックします。

詳細

ここでは、選択したトンネルブローカーに対して他のサーバアドレスを指定できます。

設定を保存するには*適用*をクリックします。

6.5 スタティックルート

ネットワークに接続されたすべてのコンピュータは、ルーティングテーブルを使用して、発信したデータパケットを宛先に届くように送信するためのパスを決定します。たとえば、ルーティングテーブルには、宛先アドレスがローカルネットワーク上にあるか、またはデータパケットをルータに転送するべきかどうか、といった情報が含まれています。ルータを使用する場合は、テーブルには、どのルータをどのネットワークに使用するかという情報が含まれます。

Sophos UTMのルーティングテーブルには、標準スタティックルートとポリシールートという2種類のルートを追加できます。スタティックルートでは、ルーティングターゲットはパケットの宛先アドレスだけで決定されます。ポリシールートでは、送信元インタフェース、送信元アドレス、サービス、あるいは宛先アドレスに基づいてルーティングを決定できます。

注 – UTM のインタフェースに接続されたネットワークに対して、追加ルートを設定する必要はありません。また、デフォルトルートも設定する必要はありません。これらのルートはシステムが自動的に追加します。

6.5.1 標準スタティックルート

システムに直接接続されたネットワークについては、システムがルーティングエントリをルーティングテーブルに自動的に挿入します。特定ネットワーク経由でアクセスする追加ルータを使用する場合は、エントリを手動で入力する必要があります。直接接続されていないネットワークへのルートで、コマンドまたは設定ファイルを使ってルーティングテーブルに挿入されるものをスタティックルートと呼んでいます。

標準スタティックルートを追加するには、以下の手順に従います。

1. ***標準スタティックルート*タブで、*新規スタティックルート*をクリックします。**
   *スタティックルートを追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   ルートタイプ: 次のルートタイプを使用できます。

   - *インタフェースルート*: パケットは特定のインタフェース上で送信されます。これは2つの状況で役立ちます。1つ目は、ゲートウェイの IP アドレスが不明になるダイナミック（動的）インタフェース（PPP）上でルーティングする場合です。2番目は、直接接続され

たネットワークの外側にゲートウェイがあるデフォルトルートを定義する場合です。

- ゲートウェイルート: パケットは特定のホスト(ゲートウェイ)へ送信されます。
- ブラックホールルート: パケットは確認なしで廃棄されます。これはOSPFまたは他のダイナミックアダプティブ(動的適応型の)ルーティングプロトコルでルーティングループやルートフラッピングなどを回避する場合に役に立ちます。

ネットワーク: UTMがインターセプトするデータパケットの宛先ネットワークを選択します。

インタフェース: データパケットがUTMを通過するインタフェースを選択します(ルートタイプに*インタフェースルート*を選択した場合のみ使用可能)。

ゲートウェイ: UTMがデータパケットを転送するゲートウェイ/ルータを選択します(ルートタイプに*ゲートウェイルート*を選択した場合のみ使用可能)。

コメント(オプション): 説明などの情報を追加します。

3. **オプションで、次の詳細設定を行います。**
   メトリック: 0～4294967295の整数でメトリック値を指定します。デフォルトは5です。メトリック値は同じ宛先へのルートを区別して優先するために使用されます。低いメトリック値の方が、高いメトリック値よりも優先されます。IPsecルートのメトリックは自動的に0に設定されます。

4. ***保存*をクリックします。**
   新しいルートが*標準スタティックルート*リストに表示されます。

5. **ルートを有効にします。**
   トグルスイッチをクリックして、ルートを有効にします。

ルートを編集または削除するには、対応するボタンをクリックします。

6.5.2 ポリシールート

ルータがデータパケットを受信すると、通常はパケットの宛先アドレスに基づいて転送先を決定し、この宛先アドレスを使用してルーティングテーブルのエントリが検索されます。ただし、他の基準に基づいてパケットを転送することが必要な場合もあります。ポリシベースのルーティングでは、お客様のポリシに従ってデータパケットをフォワーディング(転送)またはルーティングできます。

ポリシルートを追加するには、以下の手順に従います。

1. ***ポリシルート*タブで、*新規ポリシルート*をクリックします。**
   *ポリシールートを追加*ダイアログボックスが開きます。

2. **次の設定を行います。**

位置 : 位置番号。これによってポリシルートの優先順位が定義されます。番号が小さいほど優先順位が高くなります。ルートは昇順に照合されます。あるルートが一致すると、それ以降、それより大きい番号のルートは評価されません。

ルートタイプ: 次のルートタイプを使用できます。

- インタフェースルート: パケットは特定のインタフェース上で送信されます。これは2つの状況で役立ちます。1つ目は、ゲートウェイの IP アドレスが不明になるダイナミック(動的)インタフェース(PPP)上でルーティングする場合です。2番目は、直接接続されたネットワークの外側にゲートウェイがあるデフォルトルートを定義する場合です。
- ゲートウェイルート: パケットは特定のホスト(ゲートウェイ)へ送信されます。

送信元インタフェース: ルーティングされるデータパケットが到着したインタフェース。*すべて*を設定すると、すべてのインタフェースが該当することになります。

送信元ネットワーク: ルーティングされるデータパケットの送信元ネットワーク。*すべて*を設定すると、すべてのネットワークが該当することになります。

サービス: ルーティングされるデータパケットに一致するサービス定義。ドロップダウンリストには、定義済みのサービスとお客様が定義されたサービスがすべて含まれます。これらのサービスにより、どのようなトラフィックを処理するかを精密に指定できます。*すべて*を設定すると、プロトコル、送信元、および宛先ポートのあらゆる組み合わせに一致します。

宛先ネットワーク: ルーティングされるデータパケットの宛先ネットワーク。*すべて*を設定すると、すべてのネットワークが該当することになります。

ターゲットインタフェース: データパケットの送信先インタフェース(ルートタイプとして*インタフェースルート*を選択したときのみ使用可能)。

ゲートウェイ : ゲートウェイがデータパケットを転送するゲートウェイ/ルータを選択します(ルートタイプに*ゲートウェイルート*を選択した場合のみ使用可能)。

コメント(オプション) : 説明などの情報を追加します。

3. ***保存*をクリックします。**
   新しいポリシが*ポリシルート*リストに表示されます。

4. **ルートを有効にします。**
   トグルスイッチをクリックして、ルートを有効にします。

ルートを編集または削除するには、対応するボタンをクリックします。

6.6 OSPF

OSPF（Open Shortest Path First）プロトコルは、リンクステート型の階層ルーティングプロトコルであり、大規模な自律システム(AS)ネットワーク内で主に使用されます。Sophos UTMは OSPF バージョン 2 をサポートしています。他のルーティングプロトコルと比べ、OSPFはルーティングメトリックとしてコストを使用しています。OSPF対応インタフェースのコストは、特定のインタフェース経由でパケットを送信するときに必要なオーバーヘッドを示します。インタフェースのコストは、そのインタフェースの帯域幅に反比例します。そのため、帯域幅が大きいと、コストが小さくなります。たとえば、10 Mbpsのイーサネット回線より56 Kbpsのシリアル回線の方がオーバーヘッドが増え（コストが高くなり）、遅延時間が長くなります。

接続されたネットワークのコストの計算方法は、OSPF仕様には指定されておらず、ベンダーに任されています。そのため、独自の計算式を定義することができます。ただし、コストがすでに定義されている他のネットワークとOSPFネットワークが隣接している場合、同じ計算ベースを適用することをお勧めします。

デフォルトでは、インタフェースのコストは帯域幅に基づいて計算されます。たとえば、Cisco の場合、10^8 をインタフェースの帯域幅 (bps) で割ってコストを計算しています。この計算式を使用すると、10 Mbps のイーサネット回線を経由する場合のコストは $10^8/10000000 = 10$ となります。一方、1.544 Mbps の回線 (T1) では、$10^8/1544000 = 64$ となります (コストの計算では、小数点以下を切り捨てます)。

6.6.1 グローバル

*インタフェース& ルーティング > ダイナミックルーティング OSPF > グローバル*タブでは、OSPFの基本設定を行うことができます。OSPF機能を有効にする前に、OSPFエリアを1つ以上設定しておく必要があります（*エリア*タブ）。

警告 – Sophos UTMのOSPF機能を設定するためには、OSPF プロトコルを熟知している技術的に熟練した経験豊富な管理者が必要です。ここでの設定オプションについての解説は、OSPFプロトコルについて完全に理解するために十分であるとは言えません。そのため、この機能は慎重に使用することをお勧めします。設定を誤ると、ネットワークが動作不可能になる場合があります。

OSPFを設定するには、次の手順に従ってください。

1. *エリア*タブで、**OSPF エリアを 1つ以上作成します。**
2. *グローバル*タブで、**OSPFを有効化します。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、*ルーター*エリアが編集可能になります。
3. **ルータIDを入力します。**
   Sophos UTMデバイスを他のOSPFルータから識別するための独自のルータIDを入力します。
4. *適用*をクリックします。
   設定が保存されます。

   トグルスイッチが緑色に変わります。

OSPF を無効にするには、トグルスイッチをクリックします。

6.6.2 エリア

OSPFネットワークは、複数のエリアに分割されます。エリアとは、ネットワークの残りの部分のために情報をひとまとめにできるルータの論理グループです。エリアの識別名は、10進ドット表記の32ビットIDであり、IPアドレスの表記法と似ています。

OSPFエリアは全部で6種類あります。

- *バックボーン*: IDが0(または`0.0.0.0`)のエリアはOSPFネットワークバックボーンに予約されており、OSPFネットワークの中核となります。他のすべてのエリアがこのエリアに接続されます。
- *標準*: 標準エリアは`0.0.0.1`)～4,294,967,295(または`255.255.255.255`)という一意のID範囲を持ちます。ノーマルエリアは、*エリア境界ルータ*(ABR)を介して外部ルートを双方向的にフラッディングして処理します。外部ルートとは、他のルーティングプロトコルからOSPF内に配布されたルートとして定義されます。
- *スタブ*: 通常、Stubエリアは外部ネットワークと直接接続されません。外部ネットワークへのすべてのトラフィックは*エリア境界ルータ*(ABR)を介してルーティングする必要があるため、Stubエリアに外部ルートをインジェクトする必要はありません。そのため、スタブエリアは外部ネットワークにトラフィックを送信する外部ルートにとってデフォルトルートの代わりとなります。
- *スタブサマリなし*: *Stub No-Summary*または*Totally Stubby Area*はスタブエリアと似ていますが、このエリアはいわゆるサマリルートを許可しません。つまり、タイプ3のサマリリンクステートアドバタイズメント(LSA)を拒絶し、エリアに入ってこないようにします。

- **NSSA**：not-so-stubby area（NSSA）は、Stubエリアとは違い、外部接続をサポートできます。NSSAはバーチャルリンクをサポートしない点に注意が必要です。
- **NSSA**サマリなし：*NSSAサマリなし*はNSSAと似ていますが、このエリアはいわゆるサマリルートを許可しません。つまり、タイプ3のサマリリンクステートアドバタイズメント（LSA）を拒絶し、エリアに入ってこないようにします。

OSPFエリアを作成するには、次の手順に従います。

1. ***エリア*タブで*新規OSPFエリア*をクリックします。**
   *OSPFエリアの追加*ダイアログボックスが開きます。
2. **次の設定を行います。**
   名前：エリアを説明する名前を入力してください。

   エリア**ID**：エリアのIDを10進ドット表記で入力します（たとえばノーマルエリアは`0.0.0.1`、バックボーンエリアは`0.0.0.0`）。

   エリアタイプ：エリアタイプ（説明は前述）を選択し、該当するエリアに割り当てられるネットワークの特徴を指定します。

   認証タイプ：エリア内のインタフェースを介して送受信されるすべてのOSPFパケットに対して使用する認証タイプを選択します。次の認証タイプを使用できます。

   - **MD5**：選択すると、MD5認証が有効になります。MD5（Message-Digest algorithm 5）とは、128ビットのハッシュ値を使用する一般的な暗号ハッシュ関数です。
   - プレーンテキスト：選択すると、プレーンテキスト認証が有効になります。パスワードはネットワーク上を平文の形で伝送されます。
   - オフ：選択すると、認証が無効になります。

   インタフェース経由で接続：OSPF対応インタフェースを選択します。ここでOSPF対応インタフェースを指定するためには、事前に*インタフェース*タブでこのインタフェースを作成しておく必要があります。

   バーチャルリンクを使用：OSPF*自律システム*（AS）内のすべてのエリアは、バックボーンエリア（エリア0）に物理的に接続されている必要があります。物理的な接続が不可能な場合には、バーチャルリンクを使用して、非バックボーンエリアを介してバックボーンに接続できます。*仮想リンクの接続*ボックスに、バーチャルリンクのネイバーに関連付けられたルータIDを10進ドット表記で入力します（`10.0.0.8`など）。

   コスト：このエリアでデータパケットを送受信するコスト。有効な値は1～65535の範囲内です。

   コメント（オプション）：説明などの情報を追加します。

3. *保存*をクリックします。
   新しいエリア定義が*エリア*タブに表示されます。

OSPFエリアを編集または削除するには、対応するボタンをクリックします。

ライブログを開く: OSPFライブログには、OSPFインタフェースでのすべてのアクティビティが記録されます。ボタンをクリックして、新しいウィンドウでライブログを開きます。

6.6.3 インタフェース

*インタフェース& ルーティング > ダイナミックルーティング (OSPF) > インタフェース*タブでは、OSPFエリア内で使用するインタフェースの定義を作成できます。それぞれの定義には、OSPF対応インタフェースに固有の複数のパラメータがあります。

OSPFインタフェース定義を作成するには、次の手順に従います。

1. **インタフェースタブで新規OSPFインタフェースをクリックします。**
   *OSPFインタフェースの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前: このインタフェースを説明する名前を入力してください。

   インタフェース: このOSPFインタフェース定義と関連付けるインタフェースを選択します。

   認証タイプ: このインタフェースを介して送受信されるすべてのOSPFパケットに対して使用する認証タイプを選択します。次の認証タイプを使用できます。

   - **MD5**: 選択すると、MD5認証が有効になります。MD5(Message-Digest algorithm 5)とは、128ビットのハッシュ値を使用する一般的な暗号ハッシュ関数です。
   - プレーンテキスト: 選択すると、プレーンテキスト認証が有効になります。パスワードはネットワーク上を平文の形で伝送されます。
   - オフ: 選択すると、認証が無効になります。

   メッセージダイジェスト: このOSPFインタフェースに対してMD5認証が使用されることを示すメッセージダイジェスト(MD)を選択します。ここでメッセージダイジェストを選択するためには、事前に*メッセージダイジェスト*タブでそのメッセージダイジェストを作成しておく必要があります。

   コスト: このインタフェースでデータパケットを送信するコスト。有効な値は1～65535の範囲内です。

詳細オプション(オプション):このチェックボックスにチェックを入れると、追加の設定オプションが表示されます。

- **Hello間隔:** Sophos UTMがこのインタフェースを介して*Hello*パケットを送信する間隔(秒)を指定します。デフォルト値は10秒です。
- **再送間隔:** LSA(リンクステートアドバタイズメント)を受け取ったという確認応答のACKがインタフェースに届かなかったときに、インタフェースがLSAを再送する間隔(秒)を指定します。デフォルト値は5秒です。
- **Dead間隔:** Sophos UTMがこのインタフェースを介して*Hello*パケットの受信を待機する期間(秒)を指定します。デフォルト値は40秒です。原則的に、*Dead間隔*の値は*Hello間隔*の値の4倍の長さにします。
- **優先順位:** ルータの優先順位を1～255の範囲の8ビット値で指定します。この値は、特定のネットワークの指名ルータ(DR)を決定するために主に使用されます。優先順位が高いルータほど、指定ルータにふさわしい候補と見なされます。値を0に設定すると、そのルータは指定ルータの候補から外されます。デフォルト値は1です。
- **送信遅延:** インタフェースでLSUパケット送信に予想される期間(秒)を指定します。範囲は1～65535秒で、デフォルト値は1です。

コメント(オプション):説明などの情報を追加します。

3. ***保存*をクリックします。**
   OSPFインタフェース定義が*インタフェース*タブに表示されます。

OSPFインタフェースを編集または削除するには、対応するボタンをクリックします。

ライブログを開く: OSPFライブログには、OSPFインタフェースでのすべてのアクティビティが記録されます。ボタンをクリックして、新しいウィンドウでライブログを開きます。

6.6.4 メッセージダイジェスト

*インタフェース& ルーティング > ダイナミックルーティング OSPF > メッセージダイジェスト*タブでは、いわゆるメッセージダイジェストキーを生成することができます。メッセージダイジェスト鍵は、OSPFでMD5認証を有効にするために必要です。MD5認証では、パスワードを使用してメッセージダイジェストを生成します。これはデータパケットとパスワードの128ビットのチェックサムです。メッセージダイジェストは、パスワードと関連付けられた鍵IDとともにデータパケットで送信されます。

> 注 – 受信側ルータは、同じメッセージダイジェストキーで設定されていなければなりません。

メッセージダイジェストキーを作成するには、次の手順に従います。

1. *メッセージダイジェスト*タブで*新規メッセージダイジェストキー*をクリックします。
   *メッセージダイジェストキーの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   ID: このメッセージダイジェストキーのキーIDを入力します。範囲は1～255です。

   MD5キー: 関連するパスワードを入力します。最大16文字の英数字から成る文字列にする必要があります。

3. *保存*をクリックします。
   新しいキーが*メッセージダイジェスト*リストに表示されます。

ダイジェストキーを編集または削除するには、対応するボタンをクリックします。

6.6.5 デバッグ

*インタフェース& ルーティング > ダイナミックルーティング OSPF > デバッグ*タブでは、関連OSPFパラメータについての詳細情報が別のブラウザウィンドウで表示されます。次の情報が含まれています。

- **OSPF**ネイバの表示: OSPFネイバ情報をインタフェース単位で表示するために使用します。
- **OSPF**ルートの表示: ルーティングテーブルの現在の状態を表示するために使用します。
- **OSPF**インタフェースの表示: OSPF関連のインタフェース情報を表示するために使用します。
- **OSPF**データベースの表示: 特定ルータのOSPFデータベースに関連する情報を一覧表示するために使用します。
- **OSPF**境界ルータの表示: ABR *エリア境界ルータ*とASBR *自律システム境界ルータ*への内部OSPFルーティングテーブルのエントリを表示するために使用します。

6.6.6 詳細

*インタフェースとルーティング > OSPF > 詳細*タブには、OSPFに関連する追加の設定オプションがあります。これらは、OSPF以外のドメインからOSPFドメインへのルーティング情報の再配布に関連するものです。

注 – ポリシルートを再分配することはできません。

直接接続されたネットワークを再配布：直接接続されているネットワークのルートを再配布する場合は、これを選択します。デフォルトのメトリック（コスト）値は10です。

スタティックルートを再配布：スタティックルートを再分配する場合は、これを選択します。

> 注 – IPsecトンネルを再配分するためには*ストリクトルーティング*を無効化する必要があります（接続の章を参照）。

IPsecの再配布：IPsecルートを再配布したい場合に選択します。*インタフェースにバインド*オプションは無効にしてください。

SSL VPNを再配布：SSL VPNを再分配する場合は、これを選択します。デフォルトのメトリック（コスト）値は10です。

BGPを再配布：BGPルートを再分配する場合は、これを選択します。デフォルトのメトリック（コスト）値は10です。

デフォルトルートを配布：デフォルトルートをOSPFドメインに再配布したい場合は、これを選択します。デフォルトのメトリック（コスト）値は25です。

> 注 – デフォルトルートは、`0.0.0.0/0`へのルートの有無を問わずOSPFドメインにアドバタイズされます。

インタフェースリンク検出：インタフェースリンクが検出された場合にのみインタフェースのルートをアナウンスする場合は、これを選択します。

6.7 BGP

Border Gateway Protocol（BGP）とは、主にインターネットサービスプロバイダ（ISP）により、複数の自律システム（AS）間（つまりISP間）の通信を可能にするために使用されるルーティングプロトコルで、インターネットのバックボーンになっています。自律システムは、1つ以上のISPにより制御され、内部ルーティングプロトコル（IGPなど）により接続されたIPネットワークの集合です。BGPはパスベクトル型プロトコルと形容されており、IGPと異なり、パス、ネットワークポリシ、ルールセットに基づいてルーティングを決定します。このために、ルーティングプロトコルではなく、到達可能性プロトコルとみなすことができます。

各ISP（または他のネットワークプロバイダ）は、ネットワーク上でそれぞれのISPを識別するために正式に登録された自律システム番号（ASN）を持つ必要があります。ISPは内部的に複数の自律システムをサポートすることができますが、インターネットにとってはルーティングプロトコルのみが

重要になります。64512～65534の範囲の番号のASNはプライベートで、内部でのみ使用することができます。

BGPは伝送プロトコルとしてTCPをポート179で使用します。

1つのASのルータ間でBGPを使用する場合は、内部BGP（iBGP）と呼ばれ、異なるASのルータ間でBGPを使用する場合は外部BGP（eBGP）と呼ばれます。

eBGPの利点は、ルーティングループを防止することで、IPパケットがASを2度通過することがありません。これは、特定ネットワークセグメントに到達するためにIPパケットが通過する必要のあるすべてのASの全リストをeBGPルータが持つことで可能になります。ルータは送信時に、近隣のeBGPルータとこの情報を共有し、近隣のeBGPルータも必要に応じてそれぞれのルーティングリストを更新します。eBGPルータが既にこのような更新リストに存在することを検出した場合、再度リストに追加されることはありません。

6.7.1 グローバル

BGP > *グローバル*ページでは、UTMに対してBGPを有効または無効にすることができます。

1. **BGP を有効にするには、*ネイバー*ページで 1つ以上のネイバーを登録しておく必要があります。**

2. ***グローバル*ページで、BGPを有効化します。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、*BGP システム*セクションが編集可能になります。

3. **次の設定を行います。**
   AS番号：システムの自律システム番号（ASN）を入力します。

   ルーターID：ルーターIDとしてIPv4アドレスを入力します。これはセッションの初期化中にネイバーに送信されます。

   ネットワーク:システムからネイバーにアナウンスするネットワークを追加または選択します。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

   注 – アナウンス対象のネットワークは、物理的または仮想のインタフェースに割り当てられている必要があります。存在しないIPへのアクセス要求は、BGPネイバーとUTMとの間でループします。

4. ***適用*をクリックします。**

トグルスイッチが緑色になり、BGPが有効になります。しばらくすると、*BGP概観*セクションにステータス情報が表示されます。

6.7.2 システム

BGP > *システム*ページでは、複数の自律システムの環境を作成できます。

注 – このページは、*詳細*ページで複数のASの使用を有効にしている場合にのみアクセスできます。

新しいBGPシステムを作成するには、次の手順に従います。

1. ***システム*ページで*新規BGPシステム*をクリックします。**
   *BGPシステムを追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前 : システムを説明する名前を入力します。

   ASN : システムの自律システム番号(ASN)を入力します。

   ルーター**ID** : ルーターIDとしてIPv4アドレスを入力します。これはセッションの初期化中にネイバーに送信されます。

   ネイバー: このシステムのASに属するネイバーのチェックボックスにチェックを入れます。最初に*ネイバー*ページでネイバーを登録する必要があることに注意してください。

   ネットワーク: システムからアナウンスするネットワークを追加または選択します。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

   インストールルート: このオプションはデフォルトで有効になっています。BGPルータにルートを把握させる一方で、BGPルーティングプロセスにはあまり関与させたくない場合にのみ、無効にしてください。複数のASシステムでこのオプションが選択されている場合、フィルタリストを作成して重複ネットワークが存在することがないようにしてください。そうしないと、同一ネットワークのルーティング動作が定義されなくなります。

3. ***保存*をクリックします。**
   システムが*システム*リストに表示されます。

6.7.3 ネイバー

*BGP > ネイバー*ページでは、1つ以上のBGPネイバールータを登録できます。ネイバールータ(ピアルータ)は、複数の自律システム(AS)間か1つのAS内で接続を構築します。2つのネイバー間での最初の通信時に、それぞれのBGPルーティングテーブルが交換されます。その後は、ルーティングテーブルの変更に対する更新情報を相互に送信します。接続が確立していることを確認するためにキープアライブパケットを送信します。エラーが発生した場合には、通知パケットが送信されます。

BGPのポリシルーティングでは、受信ポリシと送信ポリシが異なります。このため、受信トラフィックと送信トラフィックに別々のルートマップとフィルタリストを定義して適用することができます。

*グローバル*ページでBGPを有効化できるようにするには、1つ以上のネイバールータを作成する必要があります。

新しいBGPネイバーを登録するには、次の手順に従います。

1. ***ネイバー*ページで*新規BGPネイバー*をクリックします。**
   *BGPネイバーを追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:BGPネイバールータの名前を入力します。

   ホスト: ネイバーのホスト定義を追加または選択します。定義されたIPアドレスが、UTMから到達できる必要があります。定義を追加する方法は、*定義とユーザ > ネットワーク定義 > ネットワーク定義*ページで説明しています。

   リモートASN:ネイバーの自律システム番号(ASN)を入力します。

   認証:ネイバーで認証を必要とする場合、ドロップダウンリストから*TCP MD5シグニチャ*を選択し、ネイバーに設定されているパスワードを入力します。

3. **必要に応じて次の詳細設定を行います。**
   受信/送信ルート: ルートマップを定義している場合、ここで選択できます。*受信ルート*または*送信ルート*を使用してルートマップを受信アナウンスメントまたは送信アナウンスメントに適用するかどうかを定義します。

   受信/送信フィルタ: フィルタリストを定義している場合、ここで選択できます。*受信フィルタ*または*送信フィルタ*を使用してフィルタを受信アナウンスメントまたは送信アナウンスメントに適用するかどうかを定義します。

Next-Hop-Self：iBGPネットワークでは、ルータが外部eBGPネットワークを内部的にアナウンスした場合、直接的な外部接続を持たないiBGPルータはそのネットワークへのパケットのルーティング方法を把握していません。このオプションを選択すると、eBGPルータは外部ネットワークに到達するための次のホップとして自らをアナウンスします。

マルチホップ：場合によって、Ciscoルータは、2つの外部ピアの直接接続を許可しないサードパーティのルータとして、eBGPを実行することができます。この接続を実現するには、eBGPマルチホップを使用します。eBGPマルチホップでは、直接接続がない2つの外部ピアの間でネイバー接続が可能です。マルチホップが使えるのはeBGPであり、iBGPでは使用できません。

Soft-Reconfiguration：デフォルトで有効化されています。このオプションにより、ネイバーから送信される更新を保存することができます。

デフォルトルート生成：ネイバーにデフォルトルート0.0.0.0で送信します。ネイバーは、ルーティングテーブルに存在しないネットワークに到達するために必要な場合にのみ、このルートを使用します。

ウェイト：Cisco専用のオプションです。このネイバーから学習したすべてのルートの汎用ウェイトを設定します。設定できる値は0～65535です。ウェイトが最も高いルートが、特定ネットワークに到達するために優先されます。ここで指定されたウェイトは、ルートマップのウェイトを上書きします。

4. ***保存*をクリックします。**
   ネイバーが*ネイバー*リストに表示されます。

6.7.4 ルートマップ

BGPでは、ルートマップとは、ルートの再配布条件を設定し、ポリシルーティングを有効化するためのコマンドを指します。*BGP > ルートマップ*ページでは、特定ネットワークのルートマップを作成し、メトリック、ウェイト、プリファレンスの値を設定することができます。

どのルートを取るかを決定するベストパスアルゴリズムは次のように機能します。

1. ウェイトをチェックします。*
2. ローカルプリファレンスをチェックします。*
3. ローカルルートをチェックします。
4. ASパス長をチェックします。

5. 送信元をチェックします。

6. メトリックをチェックします。*

これはあくまでも簡素化した説明です。ベストパスの計算は非常に複雑であるため、詳しくはインターネット上の関連資料などを参照してください。

アスタリスク(*)が付いた項目は直接設定することができます。

BGPルートマップを作成するには、次の手順に従います。

1. ***ルートマップ*ページで*新規BGPルートマップ*をクリックします。**
   *BGPルートマップを追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前 : ルートマップを説明する名前を入力します。

   マッチ基準 : ルートマップの一致対象を特定ルータのIPアドレスにするか、AS全体のIPアドレスにするかを選択します。

   - **IP**アドレス: *ネットワーク*ボックスに、フィルタを適用するホストまたはネットワークを追加または選択します。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

   - **AS**番号 : *AS正規表現*ボックスに、フィルタを適用するAS番号を定義するためのBGP正規表現を指定します。例: `_100_`を指定すると、AS100を通過するすべてのルートが一致します。

   ネットワーク:ルートマップを適応するネットワーク/ホストを追加または選択します。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

   メトリック: 既定では、ルータがルートメトリックを動的に学習します。しかし、0～4294967295の整数を使用して独自のメトリック値を設定できます。低いメトリック値の方が、高いメトリック値よりも優先されます。

   加重 : ベストパスの選択に使用されます。これは特定ルータに対して指定するもので、伝達されません。同じ宛先に複数のルートが存在する場合、高いウェイト値のルートが優先されます。ウェイトは最初に一致したASパスに基づき、0～4294967295の整数で設定できます。

   > 注 - ネイバーにウェイトが設定されている場合、指定されたネットワークへのルートが一致すると、このウェイトによってルートマップのウェイトが上書きされます。

プリファレンス: ローカルASのすべてのルータのみに送信されるASパスのプリファレンス値を設定することができます。プリファレンス(ローカルプリファレンス)は、AS外の特定ネットワークに到達するときに優先するパスをAS内のルータに指示するものです。0～4294967295の整数で設定でき、デフォルトは100です。

ASプリペンド: ASパスのプリペンドは、特定ルートを回避する上でプリファレンス設定が何らかの理由により充分でない場合に使用されます(メインルートが使用できない場合にのみ取るべきバックアップルートなど)。これにより、自らのAS番号を繰り返すことで(`65002 65002 65002`など)、ASパス属性を拡張することができます。BGPルート選択では、最も短いASパスが優先されるため、この選択に影響が及びます。ASプリペンドが設定されたルートマップを意図したとおりに機能させるには、ネイバーの*送信ルート*フィールドでルートマップを選択する必要があることに注意してください。

3. ***保存*をクリックします。**
ルートマップが*ルートマップ*リストに表示されます。

これで、ネイバー定義にルートマップを使用することができます。

6.7.5 フィルタリスト

*BGP > フィルタリスト*ページでは、IPアドレスまたはAS番号に基づいてネットワーク間のトラフィックを制御するために使用するフィルタリストを作成できます。

フィルタリストを作成するには、次の手順に従います。

1. ***フィルタリスト*ページで*新規BGPフィルタリスト*をクリックします。**
*BGPフィルタリストを追加*ダイアログウィンドウが開きます。

2. **次の設定を行います。**
名前:フィルタリストを説明する名前を入力します。

*フィルタ*条件:フィルタの一致対象を特定ルータのIPアドレスにするか、AS全体のIPアドレスにするかを選択します。

- **IP**アドレス: *ネットワーク*ボックスに、フィルタを適用するホストまたはネットワークを追加または選択します。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

- **AS**番号: *AS正規表現*ボックスに、フィルタを適用するAS番号を定義するためのBGP正規表現を指定します。例: `_100_`を指定すると、AS100を通過するすべてのルートが一致します。

ネットワーク: 特定ネットワークに関する情報を拒否または許可するネットワーク/ホストを追加または選択します。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

アクション: ドロップダウンリストから、フィルタが一致した場合に取るアクションを選択します。トラフィックを拒否するか許可することができます。

- 否認: *ネイバー*ページの*受信フィルタ*フィールドで特定ネイバーのネットワークを拒否した場合、UTMではそのネットワークのアナウンスメントを無視します。*送信フィルタ*フィールドで特定ネイバーのネットワークを拒否した場合、UTMではそのネットワークのそのネイバーにアナウンスメントを送信しません。
- 許可: *ネイバー*ページの*受信フィルタ*フィールドで特定ネイバーのネットワークを許可した場合、UTMではそのネットワークのみのアナウンスメントを受信します。*送信フィルタ*フィールドで特定ネイバーのネットワークを許可した場合、UTMではそのネットワークのそのネイバーのみにアナウンスメントを送信し、*グローバル*または*システム*ページで定義した他のネットワークには送信しません。

3. ***保存*をクリックします。**
   フィルタリストが*フィルタリスト*リストに表示されます。

これで、ネイバー定義にフィルタリストを使用することができます。

6.7.6 詳細

BGP > *詳細*ページでは、BGPの追加設定を行ったり、BGPデバッグ情報ウィンドウにアクセスすることができます。

複数の自律システムの許可

複数ASを許可: 複数ASを設定するには、このチェックボックスにチェックを入れます。これで、複数ASを追加できる*システム*ページが有効になります。同時に、*グローバル*ページの*BGPシステム*セクションが無効になり、*グローバル*ページにすべてのASの情報が表示されます。

厳密IPアドレスマッチ

厳密IPアドレスマッチ: IPアドレスの完全な一致を行うには、このチェックボックスにチェックを入れます。例: 10.0.0.0/8は10.0.0.0/8と一致しますが、10.0.1.0/24には一致しません。

マルチパスルーティング

通常、コストが等しい複数のルートが存在する場合でも、使用できるルートパスは1つのみです。これを選択すると、8つまでの等価ルートを同時に使用できるようになります。これにより複数のイン

タフェース間でのロードバランシングが可能になります。

注 – 複数のインタフェース間でのバランシングは、同一のASNを使用するネイバーについてのみ有効となります。

BGPデバッグ

このセクションには、3つのデバッグ情報ウィンドウがあります。ボタンをクリックしてウィンドウを開きます。各ボタンの名前は、通常コマンドラインで呼び出すBGPコマンドに対応しています。ボタンをクリックすると、ウィンドウにそのコマンドの結果がコマンドライン出力形式で表示されます。

IP BGPネイバーの表示 : UTMのネイバー情報を表示します。各ネイバーのリンク状態が*確立*となっていることを確認します。

IP BGPユニキャストの表示 : 優先パスを示す現在のBGPルーティングテーブルが表示されます。これは、メトリック、ウェイト、プリファレンスの設定とその影響の概要を確認する上で特に有益です。

IP BGPサマリの表示 : すべてのBGP接続のステータスが表示されます。この情報は、*グローバル*ページの*BGPサマリ*セクションにも表示されます。

6.8 マルチキャストルーティング PIM-SM

*インタフェース& ルーティング > マルチキャストルーティング(PIM-SM)*メニューを使用すると、ネットワーク上で使用するPIM-SM *(Protocol Independent Multicast Sparse Mode)* を設定することができます。PIM とは、複数ネットワーク内でマルチキャストパケットを動的(ダイナミック)にルーティングするためのプロトコルです。マルチキャストとは、複数のクライアントが受信するパケットをできるだけ小さいトラフィックを使用して効率的に配信するための技術です。通常、複数のクライアント宛てのパケットは、コピーされて各クライアントに個別に送信されるため、消費される帯域幅はユーザ数に応じて増大します。そのため、同じパケットを同時に要求する多数のクライアントを抱えるサーバー(コンテンツのストリーミング用サーバーなど)の場合、大量の帯域幅が必要となります。

これに対しマルチキャストは、ネットワークの各リンク経由でパケットを一度だけ送信することにより帯域幅を節約します。これを実現するために、マルチキャストでは、サーバ(送信者)からクライアント(受信者)への経路上でいつコピーを作成するかを決定するために、適切に設定されたルータを使用します。これらのルータは、PIM-SMを使用してアクティブなマルチキャスト受信者を追跡し、ルーティングの設定にこの情報を使用します。

PIM-SM通信の簡単な説明は次のようになります。送信者がマルチキャストデータの送信を開始します。送信者用のマルチキャストルータがPIM-SM経由でRPルータに登録し、RPルータは送信者のルータにJoinメッセージを送信します。マルチキャストパケットが送信者からRPルータに流れるようになります。受信者が、このマルチキャストグループのIGMPブロードキャスト経由でローカルPIM-SMルータに自己登録します。このルータは受信先用のJoin要求をRPルータに向けて送信し、RPルータはマルチキャストトラフィックを受信者に転送します。

マルチキャストは、独自のIPアドレス範囲(`224.0.0.0/4`)を持ちます。

6.8.1 グローバル

マルチキャストルーティング PIM-SM > *グローバル*タブでは、PIMを有効または無効にできます。*ルーティングデーモンの設定*エリアには、関与するインタフェースとルータのステータスが表示されます。

PIMを有効にする前に、*インタフェース*タブでPIMインタフェースとして機能するインタフェースを2つ以上定義して、*RPルータ*タブでルータを1台定義する必要があります。

PIM-SMを有効にするには、次の手順に従います。

1. ***グローバル*タブでPIM-SMを有効化します。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色に変わり、*ルーティングデーモン設定*エリアが編集可能になります。

2. **次の設定を行います。**
   *アクティブな***PIM-SM***インタフェース*: PIM-SMに使用するインタフェースを2つ以上選択します。インタフェースの設定は*インタフェース*タブで行います。

   *アクティブな***PIM-SM RP***ルータ*: PIM-SMに使用するRPルータを1つ以上選択します。RPルータの定義は*RPルータ*タブで行います。

3. ***適用*をクリックします。**
   設定が保存されます。

   トグルスイッチが緑色になり、ネットワークでPIM-SM通信が有効になりました。

設定をキャンセルするには、アンバー色のトグルスイッチをクリックします。PIM-SMを無効にするには、緑色のトグルスイッチをクリックします。

ライブログ

*ライブログを開く*ボタンをクリックすると、新しいウィンドウでPIMライブログが開きます。

6.8.2 インタフェース

*マルチキャストルーティング PIM-SM > インタフェース*タブでは、どのインタフェース上でSophos UTMマルチキャスト通信を行うかを定義することができます。

新しいPIM-SMインタフェースを作成するには、次の手順に従います。

1. ***インタフェース*タブで*新規PIM-SMインタフェース*をクリックします。**
   ダイアログボックス*PIM-SMインタフェースを追加*が開きます。

2. **次の設定を行います。**
   名前:PIM-SMインタフェースを説明する名前を入力してください。

   インタフェース:PIMおよびIGMPネットワークトラフィックを許可するインタフェースを選択します。

   DR優先順位(オプション):インタフェースの指定ルータ(DR)の優先順位を定義する番号を入力します。同じネットワークセグメント内に複数のPIM-SMルータが存在する場合、優先順位が最も高いルータがIGMP要求を受け付けます。$0 \sim 2^{32}$ の数字を使用できます。優先順位を指定しないと、デフォルトで0が使用されます。

   IGMP:サポートするIGMP *Internet Group Management Protocol* のバージョンを選択します。IGMPは、受信者がマルチキャストグループのメンバシップを確立するために使用します。

   コメント(オプション):説明などの情報を追加します。

3. ***保存*をクリックします。**
   新しいPIM-SMインタフェースがインタフェースリストに追加されます。

PIM-SMインタフェースを編集または削除するには、対応するボタンをクリックします。

6.8.3 RPルータ

ネットワーク上でマルチキャストを使用できるようにするためには、1つ以上のランデブーポイントルータ(RPルータ)を設定する必要があります。RPルータは、マルチキャスト受信者と送信者の両方から登録を受け付けます。RPルータとは、特定のマルチキャストグループのRPルータとして選ばれた通常のPIM-SMルータでもあります。どのルータがRPルータとなるかについて、すべてのPIM-SMルータが合意する必要があります。

RPルータを作成するには、次の手順に従います。

1. ***RPルータ*タブで*新規ランデブーポイントルータ*をクリックします。**
   *新規RPルータの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:RPルータを説明する名前を入力してください。

   ホスト:RPルータとして機能するホストを作成(または選択)します。

   優先順位:RPルータの優先順位を定義する数字を入力します。優先順位が一番低いRPルータに、Joinメッセージが送信されます。`0`〜`255`の数字を使用できます。優先順位を指定しないと、デフォルトで`0`が使用されます。

   マルチキャストグループプレフィックス:**RP**ルータが担当するマルチキャストグループを入力します。RPルータが複数のマルチキャストグループを担当する場合は、グループのプレフィックスを`224.1.1.0/24`のように定義できます。マルチキャストグループ(プレフィックス)は、マルチキャストアドレスの範囲内(`224.0.0.0/4`)にする必要があります。

   コメント(オプション):説明などの情報を追加します。

3. ***保存*をクリックします。**
   新しいRPルータがルータのリストに追加されます。

RPルータを編集または削除するには、対応するボタンをクリックします。

6.8.4 ルート

受信者と送信者の間に、継続的な通信ルートをセットアップする必要があります。受信者、送信者、RPルータが同じネットワークセグメント内にない場合、これらの間の通信を可能にするルートを作成する必要があります。

PIM-SMルートを作成するには、次の手順に従います。

1. ***ルート*タブで、*新規PIM-SMルート*をクリックします。**
   *PIM-SMルートの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   ルートタイプ:次のルートタイプを使用できます。

   - インタフェースルート:パケットは特定のインタフェース上で送信されます。これは2つの状況で役立ちます。1つ目は、ゲートウェイの IP アドレスが不明になるダイナミック(動的)インタフェース(PPP)上でルーティングする場合です。2番目は、直接接続されたネットワークの外側にゲートウェイがあるデフォルトルートを定義する場合です。

   - ゲートウェイルート:パケットは特定のホスト(ゲートウェイ)へ送信されます。

ネットワーク: PIMトラフィックをルーティングする宛先アドレス範囲を選択します。

ゲートウェイ: ゲートウェイがデータパケットを転送するゲートウェイ/ルータを選択します(ルートタイプに*ゲートウェイルート*を選択した場合のみ使用可能)。

インタフェース: ゲートウェイがデータパケットを転送するインタフェースを選択します(ルートタイプに*インタフェースルート*を選択した場合のみ使用可能)。

コメント(オプション): 説明などの情報を追加します。

3. ***保存*をクリックします。**
新しいPIM-SMルートがルートのリストに追加されます。

PIM-SMルートを編集または削除するには、対応するボタンをクリックします。

6.8.5 詳細

インタフェース& ルーティング > *マルチキャストルーティング PIM-SM* > *詳細*タブでは、PIMの詳細設定を構成することができます。

Shortest Path Tree(最短パスツリー)一設定

一部のネットワークでは、送信者、RP、受信者の間のPIM通信ルートは可能な限り最短のネットワークパスとはなりません。*SPTへの切り替えを有効にする*オプションを使用すると、特定のトラフィックしきい値に達したときに送信者と受信者の間の既存の通信を最短パスに切り替えて、モデレータのRPを省くことができます。

自動ファイアウォール設定

このオプションを有効にすると、指定されたマルチキャストグループにマルチキャストトラフィックを転送するために必要となるすべてのファイアウォールルールがシステムによって自動的に作成されます。

デバッグ設定

PIM-SMルーティングデーモンログに追加のデバッグ情報を表示するには、*デバッグモードを有効化*オプションを選択します。

7 ネットワークサービス

この章では、ご利用のネットワーク用にSophos UTMの複数のネットワークサービスを設定する方法を説明します。

この章には次のトピックが含まれます。

7.1 DNS

ネットワークサービス > *DNS*メニューにあるタブには、さまざまな設定オプションがあり、すべて *ドメインネームシステム* (DNS) に関連しています。DNS とは、ドメイン名 (コンピュータのホスト名) を IP アドレスに変換するために主に使用されるシステムです。

7.1.1 グローバル

許可ネットワーク

UTMを再帰的なDNSリゾルバとして使用することを許可するネットワークを指定できます。ここでは通常、内部ネットワークを選択します。

警告 – セキュリティリスクを招き、インターネットの悪用に道を開くので、決してネットワークオブジェクトで *すべて*を選択しないでください。

注 – 内部DNSサーバをActive Directoryの一部などとしてすでに起動している場合、このボックスは空のまま残します。

DNSSEC

Domain Name System Security Extensions (DNSSEC) は、セキュリティを強化するためのDNSへの拡張のセットです。公開鍵暗号を使用しているDNSルックアップレコードにデジタル署名することによって機能します。選択を解除すると、UTMは、すべてのDNS レコードを受け入れます。選択する

と、UTMは受信DNS要求のDNSSEC署名を確認します。署名ゾーンからの、正しく署名されたレコードだけを受け入れます。

> 注 – 選択すると、DNSレコードは、手動でインストールしたか、ISPによって割り当てられたDNSSEC非対応のフォワーダには拒否されます。この場合は、*フォワーダ*タブで、ボックスからDNSフォワーダを削除し、*ISPが割り当てたフォワーダを使用*チェックボックスを無効にします。

リゾルバキャッシュをクリア

DNSプロキシでは、レコードに対してキャッシュを使用します。各レコードには有効期限(TTL、生存時間)があり、この時間にレコードは削除されます。通常は1日に設定されています。ただし、キャッシュは手動で空にすることもできます(TTLが失効する前にDNSレコードの最新の変更を今すぐ有効にしたい場合など)。キャッシュを空にするには、*今すぐリゾルバキャッシュをクリア*をクリックします。

7.1.2 フォワーダ

*ネットワークサービス > DNS > フォワーダ*タブでは、いわゆるDNSフォワーダを指定できます。DNSフォワーダとは、ネットワーク上にあるDNS *ドメインネームシステム* サーバであり、外部DNS名に関するDNSクエリを当該ネットワーク外のDNSサーバに転送(フォワーディング)するために使用します。可能な限り、設定にDNSフォワーダを追加してください。DNSフォワーダは、お客様のサイトの「近く」にあり、(可能であれば)同じインターネットプロバイダが提供しているホストにする必要があります。これは「親」キャッシュとして使用されます。これにより、DNS要求の速度が飛躍的に向上します。転送を行うネームサーバを指定しないと、ゾーン情報についてのクエリ(問い合わせ)は最初にルートDNSサーバに対して行われるため、要求が完了するまで時間がかかります。

DNSフォワーダを選択するには、次の手順に従ってください。

1. **DNSフォワーダを選択します。**
   DNSフォワーダを選択または追加します。定義を追加する方法は、*定義とユーザ > ネットワーク定義 > ネットワーク定義*ページで説明しています。

   ISPが割り当てたフォワーダを使用(オプション): DNSクエリをISPのDNSサーバに転送する場合は、*ISPが割り当てたフォワーダを使用*チェックボックスにチェックを入れます。このチェックボックスにチェックを入れると、ISPによって自動的に割り当てられたすべてのフォワーダがボックスの下に一覧表示されます。

2. ***適用*をクリックします。**
   設定が保存されます。

7.1.3 リクエストルーティング

内部DNSサーバが稼働しており、DNSフォワーダに解決させたくないドメインがある場合、そのドメインへのクエリをフォワーダではなく内部サーバに処理させることができます。*ネットワークサービス > DNS > リクエストルーティング*タブで、独自のDNSサーバへのルートを定義することができます。

DNSリクエストルートを作成するには、次の手順に従います。

1. ***リクエストルーティング*タブで*新規DNSリクエストルート*をクリックします。**
   *DNSリクエストルートの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   ドメイン: 代替DNSサーバを使用したいドメインを入力します。

   ターゲットサーバ: 上記ステップで入力したドメインを解決するために使用するDNSサーバを1つ以上選択または追加します。定義を追加する方法は、*定義とユーザ > ネットワーク定義 > ネットワーク定義*ページで説明しています。

   コメント(オプション): 説明などの情報を追加します。

3. ***保存*をクリックします。**
   新しいルートが*DNSリクエストルート*リストに表示され、ただちに有効になります。

DNSリクエストルートを編集または削除するには、対応するボタンをクリックします。

7.1.4 スタティックエントリ

独自のDNSサーバをセットアップせず、ネットワーク内のいくつかのホストに対してスタティックDNSマッピングが必要な場合は、これらのマッピングを入力することができます。

UTMバージョン9.1から、この機能は*定義とユーザ > ネットワーク定義*タブに移動しています。現在は、DNS マッピングは、関与するホストと共に定義されます。

*スタティックエントリー*ボタンをクリックすると、*定義とユーザ > ネットワーク定義*タブが開きます。自動的に、スタティックエントリがあるホストだけが表示されます。リストの上部にあるドロップダウンリストを使用して、フィルタ設定を変更できます。

7.1.5 DynDNS

ダイナミックDNS(略してDynDNS)は、可変IPアドレスを持つコンピュータに静的インターネットドメイン名を割り当てることを可能にするドメインネームサービスです。それぞれのDynDNSサービスプロ

バイダのWebサイトでDynDNSサービスにサインアップし、DNSエイリアスを取得すると、アップリンクIPアドレスの変化に応じてこのエイリアスが自動的に更新されます。このサービスに登録すると、設定に必要なホスト名、ユーザ名、パスワードが提供されます。

DynDNSを設定するには、次の手順に従ってください。

1. ***DynDNSタブで、新規DynDNSをクリックします。***
   *DynDNSの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   タイプ: 次のDynDNSサービスを使用できます。

   - **DNS-O-Matic**: 特定のホスト名の代わりに一般ホスト名`all.dnsomatic.com`を使用すると、すべての設定済みサービスを一度にアップデートできます（www.dnsomatic.com/wiki/apiもご覧ください）。公式ウェブサイト:www.dnsomatic.com
   - **DNSdynamic**:公式ウェブサイト:www.dnsdynamic.org
   - **DNS Park**: 公式ウェブサイト:www.dnspark.com
   - **DtDNS**: 公式ウェブサイト:www.dtdns.com
   - **Dyn**: サービスプロバイダDynamic Network Services Inc. (Dyn)の標準DNSサービス。公式ウェブサイト:www.dyn.com
   - **Dyn** *カスタム*: サービスプロバイダDynamic Network Services Inc. (Dyn)のカスタムDNSサービス（www.dyn.com）。カスタムDNSは、主にユーザ自身が所有または登録しているドメインを使用するために設計されています。
   - **easyDNS**: 公式ウェブサイト:www.easydns.com
   - **FreeDNS**: 公式ウェブサイト:freedns.afraid.org
   - **Namecheap**: 公式ウェブサイト:www.namecheap.com
   - **No-IP.com**: 公式ウェブサイト:www.noip.com
   - **OpenDNS IP***アップデート*: 公式ウェブサイト:www.opendns.com
   - **selfHOST:** 公式ウェブサイト:www.selfhost.de
   - **STRATO AG:** 公式ウェブサイト:www.strato.de
   - **zoneedit**: 公式ウェブサイト:www.zoneedit.com

注 – *サーバ*フィールドには、UTMがIPの変更を送信するURLが表示されます。

割り当て(*FreeDNS*タイプには無効):DynDNS名を関連付けるIPアドレスを定義します。ローカルインタフェースがパブリックIPアドレスを持つ場合は、この*ローカルインタフェースのIP*を選択すると便利です。通常は、DSLアップリンクに対してこのオプションを使用します。*デフォルトルートの最初のパブリックIP*を選択する場合、インタフェースの指定は不要です。UTMデフォルトルートの最初のパブリックIPを選択する場合、インタフェースの指定は不要です。代わりに、UTMがパブリックDynDNSサーバにWWW要求を送信し、パブリックDynDNSサーバは現在使用中のパブリックIPを返します。

> 注 – FreeDNSは、常にデフォルトルートの最初のパブリックIPアドレスを使用します。

インタフェース(*ローカルインタフェースのIPのみ*):DynDNSサービスを使用するインタフェースを選択します。最も可能性が高いのは、インターネットに接続された外部インタフェースです。

レコード(*Dyn*および*FreeDNSのみ*):DynDNSサービスに使用するレコードを選択します。*A IPv4*、*A & AAA デュアルスタック*(*Dynのみ*)、および*AAAA IPv6*(*FreeDNSのみ*)から決定します。

ホスト名(*Open DNS IP*アップデートタイプ以外):DynDNSサービスプロバイダから受け取ったドメイン名を入力します(例、`example.dyndns.org`)。ここでは、特定の構文を遵守してホスト名を入力する必要はありません。ここで入力が必要な内容は、各DynDNSサービスプロバイダの要件に応じて異なります。DynDNSホスト名をゲートウェイのメインホスト名として使用することもできますが、必須ではありません。

ラベル(*Open DNS IP アップデ*ートタイプのみ):ネットワークに与えられるラベルを入力します。詳細情報は、OpenDNS Knowledgebaseを参照してください。

エイリアス(オプション、一部のタイプのみ):このボックスは、前述のメインホスト名と同じIPアドレスをポイントする追加ホスト名を入力するために使用します(`mail.example.com`、`example.com`など)。

MX(オプション、*DNS Park*、*DynDNS*、*easyDNS*タイプのみ):MX(mail exchanger)は、ホスト名で指定されたサーバ以外の特定サーバにメールを送信するために使用します。MXレコードは、特定ドメインへのメールの送信先となるホスト(サーバ)を指定するという目的のために使用します。たとえば、MXとして `mail.example.com` を指定すると、`user@example.com` 宛てのメールはホストである `mail.example.com` に配信されます。

MX優先順位(オプション、*DNS Park*タイプのみ):ドメインへのメールの配信に指定したメールサーバを優先するかどうかを示す正の整数値を入力します。数値が低いサーバーが

数値の高いサーバーよりも優先されます。DNS Parkでは、デフォルト値として5が使用され、これがほとんどの目的に適っているため、このフィールドを空白のままにすることができます。MXの優先順位の詳細な技術情報については、RFC 5321を参照してください。

バックアップ**MX**(オプション、*DynDNS*または*easyDNS*タイプのみ):*ホスト名*テキストボックスで指定したホスト名がメインMXとなる場合のみ、このチェックボックスにチェックを入れます。すると、*MX*テキストボックスのホスト名はバックアップMXとしてのみアドバタイズされます。

ワイルドカード(オプション、*DynDNS*または*easyDNS*タイプのみ):このオプションは、登録したドメインと同じIPアドレスをサブドメインのポイント先とする場合に選択します。このオプションを使用すると、ドメインにワイルドカードとしてアスタリスク(*)が追加されます(`*.example.dyndns.org`など)。これにより、`www.example.dyndns.org`などが`example.dyndns.org`と同じアドレスをポイントするようになります。

ユーザ名:DynDNSサービスプロバイダから受け取ったユーザ名を入力します。

パスワード:DynDNSサービスプロバイダから受け取ったパスワードを入力します。

コメント(オプション):説明などの情報を追加します。

3. ***保存*をクリックします。**
新しいDynDNSが*DynDNS*リストに表示されます。サービスは無効になっています(トグルスイッチは灰色)。

4. **DynDNSを有効にします。**
DynDNSサービスを有効にするには、トグルスイッチをクリックします。

   これでサービスが有効になります(トグルスイッチは緑色)。

DynDNSを編集または削除するには、対応するボタンをクリックします。

複数のDynDNSオブジェクトを同時に使用することができます。2つのホスト名のすべての設定が同じであれば、別オブジェクトを2つ作成するのではなく、*エイリアス*オプションを使用することを推奨します。

7.2 DHCP

DHCP Dynamic Host Configuration Protocol は、定義されたIPアドレスプールからクライアントコンピュータにアドレスを自動的に割り当てます。大規模ネットワークにおけるネットワーク設定を簡素化し、アドレスの衝突を防止するために設計されています。DHCP はクライアントに、IP アドレス、デフォルトのゲートウェイ情報、DNS 設定情報を割り当てます。

クライアントコンピュータの設定を簡素化し、モバイルコンピュータが複数のネットワークを問題なく行き来できるようにすることに加え、DHCPはIPアドレスに関連する問題の原因特定とトラブルシューティングもサポートします。これは、DHCPサーバ自体の設定に問題があることが多いためです。また、アドレスを必要に応じて割り当てて、不要な場合は再利用することができるため、すべてのコンピュータが同時にアクティブになっていない場合などに、アドレススペースの使用をより効率化することができます。

7.2.1 サーバ

*ネットワークサービス > DHCP > サーバ*タブで、DHCPサーバを設定できます。Sophos UTMは、接続されたネットワークだけでなく、他のネットワークに対してDHCPサービスを提供します。DHCPサーバを使用して、クライアントに基本ネットワークパラメータを割り当てることができます。独自の構成を持つそれぞれ独自のインタフェースとネットワークを取得して、複数のインタフェース上でDHCPサービスを実行できます。

注 – *オプション*タブでは、クライアントに送信する追加DHCPオプションまたは異なるDHCPオプションを定義できます。*オプション*タブで定義されるDHCPオプションは、そのスコープがグローバルに設定されていない場合、*サーバ*タブの設定を上書きします。たとえば、選択したホストのみにDHCPオプションを定義するときに、DHCPサーバに定義されたものとは異なるDNSサーバまたはリース期間を割り当てることができます。

DHCPサーバを設定するには、次の手順に従ってください。

1. ***サーバ*タブで、*新規DHCPサーバ*をクリックします。**
   *DHCPサーバの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   インタフェース: IPアドレスをクライアントに割り当てるインタフェース。すでに設定されているインタフェースのみを選択できます。

   アドレスタイプ: このオプションはIPv6をグローバルに有効にしている場合にのみ使用できます。DHCPサーバのIPバージョンを選択します。

   注 – UTM上または別のデバイス経由での*ステートフル自動設定*(管理対象フラグ)のプレフィックス広告が必要になります。*インタフェース& ルーティング > IPv6 > プレフィックス広告*タブで、プレプレフィックス広告を設定できます。

レンジの先頭/末尾：そのインタフェースのアドレスプールとして使用するIPレンジ。デフォルトで、ネットワークカードに設定されたアドレスエリアがテキストボックスに表示されます。クライアントが同じネットワーク内にある場合、レンジはインタフェースが接続されたネットワーク内にする必要があります。クライアントが別のネットワークにある場合、レンジはリレーされたDHCP要求の送信元ネットワーク内にする必要があります。

注 – 定義したDHCP IP範囲が広いほど、UTMはより多くのメモリを予約します。必ず、DHCPの範囲のサイズを必要な値に減らしてください。最大許容範囲は、9ネットワークに1つです。

DNSサーバ**1/2**：DNSサーバのIPアドレス。

デフォルトゲートウェイ（IPv4のみ）：デフォルトゲートウェイのIPアドレスです。

注 – ワイヤレスアクセスポイントとREDアプライアンスの両方で、デフォルトゲートウェイが接続先インタフェースと同じサブネット内にある必要があります。

ドメイン（オプション）：クライアントに送信されるドメイン名を入力します（例：`intranet.example.com`）。

リース期間（IPv4のみ）：DHCPクライアントがリースの更新を自動的に試行します。このリース期間中にリースが更新されない場合、IPアドレスリースの期限が切れます。ここでは、その間隔を秒数で定義できます。デフォルトは86,400秒（1日）です。最小値は600秒（10分）で、最大値は2,592,000秒（1か月）です。

有効期間（IPv6のみ）：DHCPクライアントがリースの更新を自動的に試行します。この有効期間中にリースが更新されない場合、IPアドレスリースステータスが無効になり、アドレスがインタフェースから削除され、他に割り当てられるようになります。間隔は5分から無限の間で選択できますが、有効期間は推奨期間以上にする必要があります。

推奨期間（IPv6のみ）：DHCPクライアントがリースの更新を自動的に試行します。この推奨期間中にリースが更新されない場合、IPアドレスリースステータスがデプリケート、つまり引き続き有効ではあるものの、新しい接続には使用されないようになります。間隔は、5分から無限の間で選択できます。

コメント（オプション）：説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**

WINSノードタイプ(IPv4のみ):*WINS Windows Internet Naming Service* とは、マイクロソフトがWindowsに実装した*NBNS NetBIOS Name Server* であり、NetBIOSコンピュータ名用のネームサーバおよびサービスです。WINSサーバは、コンピュータ名をIPアドレスと一致させるデータベースとして機能するため、NetBIOSを使用しているコンピュータがTCP/IPネットワークのメリットを利用できるようになります。次のWINSノードタイプを使用できます。

- 設定しない:WINSノードタイプは設定するのではなくクライアントに選択されます。
- **B**ノード **WINS**なし :Bノードシステムはブロードキャストのみを使用します。
- **P**ノード **WINS**のみ :PノードシステムはWINS(Windows name server)へのポイントツーポイントの名前問い合わせのみを使用します。
- **M**ノード ブロードキャスト後**WINS** :Mノードシステムは、まずブロードキャストしてから、ネームサーバに問い合わせを行ないます。
- **H**ノード **WINS**後ブロードキャスト :Hノードシステムは、まずネームサーバに問い合わせてから、ブロードキャストします。

WINSサーバ:選択したWINSノードタイプに応じて、このテキストボックスが表示されます。WINSサーバのIPアドレスを入力します。

スタティックマッピングされたクライアントのみ(オプション):スタティックDHCP マッピングがあるクライアントのみにDHCPサーバがIPアドレスを割り当てるようにするには、このオプションを選択します *定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*を参照)。

HTTPプロキシ自動設定の有効化: ブラウザの自動プロキシ設定用にPACファイルを提供するには、このオプションを選択します。詳細情報は、*Webプロテクション* > *フィルタリングオプション* > *その他*の章で、*プロキシの自動設定*セクションを参照してください。

> 注 – Microsoft Windowsでは現在、IPv6でHTTPプロキシの自動設定をサポートしていません。

DHCPリレー経由のクライアント(IPv4のみ):これを選択すると、DHCPサーバは接続されたインタフェースのネットワーク内に存在しないクライアントにIPアドレスを割り当てます。この場合、上に定義されたアドレスレンジは、接続されたインタフェースのネットワーク内ではなく、リレーされたDHCP要求の転送元ネットワーク内にする必要があります。

ネットマスク:リレーされたDHCP要求の転送元ネットワークのネットマスクを選択します。

4. *保存*をクリックします。

新しいDHCPサーバ定義がDHCPサーバのリストに表示され、ただちにアクティブになっています。

DHCPサーバ定義を編集または削除するには、対応するボタンをクリックします。

7.2.2 リレー

*ネットワークサービス > DHCP > リレー*タブでは、DHCPリレーを設定することができます。DHCPサービスは別のDHCPサーバによって提供され、UTMはリレーとして機能します。DHCPリレーを使用すると、ネットワークセグメントをまたいでDHCP要求および応答を転送することができます。DHCPサーバと、DHCPトラフィックが転送されるインタフェースのリストを指定する必要があります。

DHCPリレーを設定するには、次の手順に従ってください。

1. ***リレー*タブで、*DHCP リレー*を有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、*DHCP リレー設定*エリアが編集可能になります。

2. **DHCP サーバーを選択します。**

3. **関与するインタフェースを追加します。**
   DHCPサーバへのインタフェース、ならびにDHCP要求および応答を転送するクライアントネットワークへのすべてのインタフェースを追加します。

4. ***適用*をクリックします。**
   設定が保存されます。

   トグルスイッチが緑色に変わります。

設定をキャンセルするには、アンバー色のトグルスイッチをクリックします。

7.2.3 DHCPv6 リレー

*ネットワークサービス > DHCPv6 リレー*タブでは、IPv6のDHCPリレーを設定することができます。DHCPサービスは別のDHCPv6インタフェースによって提供され、UTMはリレーとして機能します。DHCPv6リレーを使用すると、ネットワークセグメントをまたいでDHCP要求および応答を転送することができます。

> 注 – DHCPv6リレーを使用するには、*インタフェース & ルーティング > IPv6 > グローバル*タブのIPv6を有効化しなければなりません。

DHCPv6リレーを設定するには、次の手順に従ってください。

1. ***DHCPv6 リレー*タブで、*DHCPv6 リレー*を有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、*DHCPv6 リレー設定*エリアが編集可能になります。

2. **関与する、クライアントと接続しているインタフェースを追加します。**
   インタフェースを、DHCPv6要求および応答を転送するクライアントネットワークに追加します。

3. **関与する、サーバと接続しているインタフェースを追加します。**
   DHCPv6サーバと接続しているインタフェースを追加します。

4. ***適用*をクリックします。**
   設定が保存されます。

   トグルスイッチが緑色に変わります。

設定をキャンセルするには、アンバー色のトグルスイッチをクリックします。

7.2.4 スタティックマッピング

一部または全部のクライアントのIPアドレスとクライアント間のスタティック(静的)マッピングを作成できます。UTM バージョン9.1から、この機能は*定義とユーザ* > *ネットワーク定義*タブに移動しています。現在は、DHCP マッピングは、関与するホストと共に定義されます。

*スタティックマッピング*ボタンをクリックすると、*定義とユーザ* > *ネットワーク定義*タブが開きます。自動的に、スタティックマッピングがあるホストだけが表示されます。リストの上部にあるドロップダウンリストを使用して、フィルタ設定を変更できます。

7.2.5 IPv4 リーステーブル

DHCPを使用すると、クライアントはIPアドレスを持つのではなく、*DHCP*サーバからIPアドレスを借りる(リースする)ことになります。これにより、アドレスを一定期間にわたって使用する許可をクライアントに与えます。

ネットワークサービス > *DHCP* > *IPv4 リーステーブル*タブにあるリーステーブルには、DHCPサーバが現在発行しているリースが、開始日付やリースの有効期限日などの情報とともに表示されます。

新しいホスト定義へのスタティックマッピングの追加

定義するホストで、既存のリースをスタティックMAC/IPマッピングのテンプレートとして使用することができます。以下の手順に従ってください。

1. 該当するリースについて、*スタティックにする*列の *スタティックにする*ボタンをクリックします。

   *スタティックにする*ダイアログウィンドウが開きます。

2. **次の設定を行います。**
   アクション: *新しいホストを作成する*を選択します。

   名前 :新しいホストを説明する名前を入力します。

   DHCPサーバ: スタティックマッピングで使用するDHCPサーバを選択します。対応するDHCP 範囲が、下のドロップダウンリストに表示されます。

   IPv4アドレス: DHCPプール範囲外のアドレスにIPアドレスを変更します。

   > 注 – リースをスタティックマッピングに変換する場合、DHCPプールの範囲外のIPアドレスに変更する必要があります。ただし、IPアドレスを変更しても、クライアントの使用するアドレスはすぐには変更されず、次にリース更新を試行するまで変更されません。

   DNSホスト名 : DNSホスト名を入力すると、ホストのスタティックDNSエントリとして使用されます。

   リバース**DNS**: ホストのIPアドレスと名前のマッピングを有効化するには、チェックボックスにチェックを入れます。同じIPアドレスに複数の名前をマッピングすることが可能ですが、1つのIPアドレスには1つの名前にしかマッピングできません。

   コメント(オプション) : 説明などの情報を追加します。

3. *保存***をクリックします。**
   設定が保存されます。

スタティックマッピングを持つ新しいホストは、*定義とユーザ* > *ネットワーク定義*タブで見つけることができます。

既存のホスト定義へのスタティックマッピングの追加

既存のリースを新しいスタティック MAC/IP マッピングのテンプレートとして使用し、ホストの定義に使用できます。以下の手順に従ってください。

1. **望ましいリースの*静的化*列の*静的化*ボタンをクリックします。**
   *スタティックにする*ダイアログウィンドウが開きます。

2. **次の設定を行います。**
   アクション: *既存のホストを使用*を選択します。

   ホスト: フォルダアイコンをクリックして、ホストを追加します。

3. **_保存_をクリックします。**
   設定が保存されます。

静的マッピングによるホストは、_定義とユーザー_ > _ネットワーク定義_タブに表示されます。

7.2.6 IPv6 リーステーブル

DHCPを使用すると、クライアントはIPアドレスを持つのではなく、_DHCP_サーバからIPアドレスを借りる(リースする)ことになります。これにより、アドレスを一定期間にわたって使用する許可をクライアントに与えます。

ネットワークサービス > _DHCP_ > _IPv6 リーステーブル_タブにあるリーステーブルには、DHCPサーバが現在発行しているリースが、開始日付やリースの有効期限日などの情報とともに表示されます。

注 – プレフィックス広告経由で付与されたリースはテーブルに表示されません。

新しいホスト定義へのスタティックマッピングの追加

定義するホストで、既存のリースをスタティックMAC/IPマッピングのテンプレートとして使用することができます。以下の手順に従ってください。

1. **該当するリースについて、_スタティックにする_ボタンをクリックします。**
   _スタティックにする_ダイアログウィンドウが開きます。

2. **次の設定を行います。**
   アクション: _新しいホストを作成する_を選択します。

   名前 : 新しいホストを説明する名前を入力します。

   DHCPサーバ: スタティックマッピングで使用するDHCPサーバを選択します。対応するDHCP 範囲が、下のドロップダウンリストに表示されます。

   IPv6アドレス: DHCPプール範囲外のアドレスにIPアドレスを変更します。

   注 – リースをスタティックマッピングに変換する場合、DHCPプールの範囲外のIPアドレスに変更する必要があります。ただし、IPアドレスを変更しても、クライアントの使用するアドレスはすぐには変更されず、次にリース更新を試行するまで変更されません。

   DNSホスト名 : DNSホスト名を入力すると、ホストのスタティックDNSエントリとして使用されます。

リバース**DNS**: ホストのIPアドレスと名前のマッピングを有効化するには、チェックボックスにチェックを入れます。同じIPアドレスに複数の名前をマッピングすることが可能ですが、1つのIPアドレスには1つの名前にしかマッピングできません。

コメント(オプション):説明などの情報を追加します。

3. ***保存*をクリックします。**
設定が保存されます。

既存のホスト定義へのスタティックマッピングの追加

既存のリースを新しいスタティック MAC/IP マッピングのテンプレートとして使用し、ホストの定義に使用できます。以下の手順に従ってください。

1. **望ましいリースの*静的化*列の*静的化*ボタンをクリックします。**
*スタティックにする*ダイアログウィンドウが開きます。

2. **次の設定を行います。**
アクション: *既存のホストを使用*を選択します。

ホスト: フォルダアイコンをクリックして、ホストを追加します。

3. ***保存*をクリックします。**
設定が保存されます。

静的マッピングによるホストは、*定義とユーザー* > *ネットワーク定義*タブに表示されます。

7.2.7 オプション

ネットワークサービス > *DHCP* > *オプション*タブを使用すると、DHCPオプションを設定することができます。DHCPオプションは、DHCPサーバによりDHCPクライアントに提供される追加設定パラメータです。

例:一部のVoIP電話の場合、DHCPサーバから必要な情報を提供するために、このページで3つの追加DHCPオプションを作成して有効にする必要があります。

- *ファイル名*:ブートファイルの名前。
- *次のサーバ*:ブートファイルを提供するTFTPサーバの名前。
- *4 タイムサーバ*:タイムサーバのIPアドレス。

DHCPオプションに異なるスコープを許可:選択したホストのみに提供するか、選択したサーバからのみとするか、グローバルにすることもできます。このため、同じホストに異なるパラメータを定義することができます。一部のDHCPオプションは、DNSサーバ(オプション6)など、*DHCP* > *サーバ*タブ

で既に定義されています。パラメータ値が一致しない場合、次の優先順位でパラメータがクライアントに提供されます。

1. スコープが*ホスト*のDHCPオプション
2. スコープが*MACプレフィックス*のDHCPオプション
3. スコープが*ベンダID*のDHCPオプション
4. スコープが*サーバ*のDHCPオプション
5. DHCPサーバパラメータ（*DHCP* > *サーバ*タブ）
6. スコープが*グローバル*のDHCPオプション

注 – DHCP要求では、DHCPクライアントが処理できるDHCPオプションに関する情報を送信します。その結果、DHCPサーバは、ここに定義されたオプションに関係なく、クライアントが理解できるDHCPオプションのみを提供します。

DHCPオプションを作成するには、次の手順に従います。

1. ***新規DHCPオプション*をクリックします。**
   *DHCPを追加オプション*ダイアログボックスが開きます。
2. **次の設定を行います。**
   アドレスタイプ（IPv6が有効な場合のみ）：DHCPオプションを作成するIPバージョンを選択します。

   コード: 作成するDHCPオプションのコードを選択します。

   注 – *ファイル名*エントリでは、そこで実行するDHCP クライアントにロードするファイルを指定できます。*次のサーバ*では、ブートサーバを定義できます。番号付きDHCPオプションコードは、RFC 2132などで定義されています。

   名前：このオプションを説明する名前を入力します。

   タイプ: コメントが *不明* のコードを選択した場合にのみ使用できます。オプションのデータタイプを選択します。データタイプには、*IPアドレス*、*テキスト*、*16進*を使用できます。選択したデータタイプに応じて、対応する下のフィールドに適切なデータを入力します。

   アドレス: このDHCPオプションでDHCPクライアントに送信するホストまたはネットワークグループのIPアドレスを選択します。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

テキスト: このDHCPオプションでDHCPクライアントに送信するテキストを入力します。

16進 : このDHCPオプションでDHCPクライアントに送信する16進値を入力します。16進数をコロンで2桁の区切ってまとめた形式で指定します(`00:04:76:16:EA:62`など)。

整数 : このDHCPオプションでDHCPクライアントに送信する整数値を入力します。

スコープ: DHCPオプションを送信する条件を定義します。

- グローバル: DHCPオプションが定義されているすべてのDHCPサーバによりすべてのDHCPクライアントに送信されます。
- サーバ: *サーバ*ボックスには、DHCPオプションを送信するDHCP サーバを選択します。ボックスには、*DHCPサーバ*タブに定義されているすべてのDHCPサーバが表示されます。
- ホスト: *ホスト*ボックスでは、DHCPオプションが提供される必要があるホストを追加または選択します。定義を追加する方法は、*定義とユーザ > ネットワーク定義 > ネットワーク定義*ページで説明しています。
- **MAC**プレフィックス: MACプレフィックスを入力します。MACアドレスが一致するすべてのDHCPクライアントにDHCPオプションが提供されます。
- ベンダ**ID** : ベンダIDまたはベンダIDのプレフィックスを入力します。この文字列に一致するすべてのDHCPクライアントにDHCPオプションが提供されます。

コメント(オプション) : 説明などの情報を追加します。

3. ***保存*をクリックします。**
   *DHCPオプション*リストに新しいDHCPオプションが表示され、直ちにアクティブになります。

DHCPオプションを編集または削除するには、対応するボタンをクリックします。

7.3 NTP

*ネットワークサービス > NTP メニューを使用すると、接続された*ネットワーク用のNTPサーバを設定することができます。*NTP (Network Time Protocol)*とは、IPネットワーク経由でコンピュータシステムのクロックの同期をとるために使用するプロトコルです。Sophos UTMの時刻の同期(*マネジメント > システム設定 > 日付と時刻*タブで設定)だけではなく、特定のネットワークがこのサービスを使用できるように明示的に許可することもできます。

特定のネットワークに対して NTP による時刻同期を有効にするには、次の手順に従ってください。

1. **NTPサーバを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、*NTPオプション*エリアが編集可能になります。

2. *許可ネットワーク***を選択します。**
   NTPサーバへのアクセスを許可するネットワークを追加または選択します。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

3. *適用***をクリックします。**
   設定が保存されます。

   トグルスイッチが緑色に変わります。

8 ネットワークプロテクション

ネットワークプロテクションSophos UTM WebAdmin の*ネットワークプロテクション統計*ページには、送信元ホストと宛先ホストの両方に対する侵入防御イベントおよび破棄されたデータパケットの概要が表示されます。各セクションには*詳細*リンクがあります。リンクをクリックするとWebAdminのそれぞれのレポーティングセクションが表示され、そこでさらなる統計情報を参照できます。

注 – *高度な脅威防御:最新のイベント*リストのプラス(+)アイコンをクリックすることで、*ネットワーク/ホスト除外*または*脅威除外*を直接追加することができます。

この章には次のトピックが含まれます。

- ファイアウォール
- ネットワークアドレス変換
- 高度な脅威防御
- 侵入防御(IPS)
- サーバロードバランシング
- ボイスオーバーIP(VoIP)
- 詳細設定

8.1 ファイアウォール

*ネットワークプロテクション > ファイアウォール*メニューを使用すると、ゲートウェイのファイアウォールルールを定義し、管理することができます。一般的に、ファイアウォールはゲートウェイの中核部分で、ネットワーク環境においてセキュリティポリシで禁止されている通信を妨げます。Sophos UTMのデフォルトのセキュリティポリシでは、ゲートウェイの他のソフトウェアコンポーネントが機能するために必要な、自動的に生成されたルールセットを除くすべてのネットワークトラフィックをブロックしてログします。ただし、自動的に生成されたルールセットは*ファイアウォール > ルール*タブには表示されません。このポリシーでは、どのデータトラフィックにゲートウェイの通過を許可するかを明確に定義する必要があります。

8.1.1 ルール

*ネットワークプロテクション > ファイアウォール > ルール*タブでは、ファイアウォールルールセットを管理できます。タブを開くと、デフォルトで、ユーザ作成のファイアウォールルールだけが表示されます。リストの上部にあるドロップダウンリストを使用すると、代わりに自動ファイアウォールルールを表示したり、両方のタイプのルールを表示したりすることを選べます。自動ファイアウォールルールは、明瞭な背景色で表示されます。自動ファイアウォールルールは、設定の1つ(例、IPsecまたはSSL接続の作成)として選択した*自動ファイアウォールルールチェックボックスに基づいてUTMが生成します。*

新規に定義したすべてのファイアウォールルールは、ルールテーブルに追加されると、デフォルトで無効になります。自動ファイアウォールルールおよび有効になっているユーザ作成のファイアウォールルールが、最初ルールが一致するまで、所定の順番で適用されます。自動ファイアウォールルールは、常にリストの一番上にあります。ユーザ作成のファイアウォールルールの処理順序は位置番号によって決まるため、位置番号によってルールの順序を変更すると、処理順序も変わります。

警告 – 1つのファイアウォールルールが一致すると、他のすべてのルールは無視されます。そのため、ルールの順番は非常に重要です。*すべて 送信元 – すべて サービス – すべて 宛先 – 許可 アクション* のようなルールは、ルールテーブルの上部には配置しないでください。このようなルールをルールテーブルの上部に配置すると、各パケットがゲートウェイを双方向に通過できるようになり、以降の他のルールはすべて無視されます。

ファイアウォールルールを作成するには、次の手順に従います。

1. ***ルール*タブで、*新規ルール*をクリックします。**
   *ルールの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   グループ: *グループ*オプションを使用すると、ルールを論理的にグループ化できます。リストの上部にあるドロップダウンリストを使用すると、ルールをグループ別にフィルタできます。グループ化は表示用のみで、ルールの一致には関係ありません。新しいグループを作成するには、<<*新規グループ*>>エントリを選択し、グループを説明する名前を*名前*に入力します。

   優先順位: ルールの優先順位を定義する位置番号。番号が小さいほど優先順位が高くなります。ルールは昇順に照合されます。あるルールが一致すると、それ以降、それより大きい番号のルールは評価されません。

送信元 : パケットの送信元のホストまたはネットワークを説明する送信元ネットワークの定義を追加または選択します。

ヒント – 定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義* ページで説明しています。

サービス: プロトコルを説明するサービス定義を追加または選択します。TCPまたはUDPの場合は、パケットの送信元および宛先ポートになります。

宛先 : パケットのターゲットホストまたはネットワークを説明する宛先ネットワークの定義を追加または選択します。

注 – 複数の送信元、サービスおよび/または宛先を選択すると、ルールは可能性がある送信元-サービス-宛先のすべての組み合わせに対して適用されます。たとえば、2つの送信元、2つのサービス、2つの宛先を含むルールは、それぞれの送信元からそれぞれの宛先で両方のサービスを使用する8つの単一ルールに相当します。

アクション: アクションは、ルールに一致したトラフィックに対する処理を説明します。次のアクションを選択できます。

- 許可 : 接続を許可し、トラフィックを送ります。
- 破棄 : このアクションが指定されたルールと一致したパケットは、警告なしでドロップされます。
- 拒否 : このアクションが指定されたルールと一致した接続要求はアクティブに拒否されます。送信者にはICMPメッセージで通知されます。

コメント(オプション) : 説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**
時間帯 : デフォルトでは、期間定義は選択されていません。つまり、ルールは常に有効です。時間帯定義を選択すると、時間帯定義で指定された期間だけルールが有効になります。詳細は、*時間帯定義*を参照してください。

トラフィックをログ: このオプションを選択すると、ログが有効になり、ルールに一致したパケットがファイアウォールログにログされます。

送信元**MAC**アドレス定義 : どのMACアドレスからパケットが送信されているかを説明する、MAC アドレスのリスト定義を選択します。選択すると、パケットがルールに一致するには、送信元のMACアドレスがこの定義でリストされている場合だけです。送信元 *すべて*と組

み合わせてMACアドレスリストを使用することはできません。MACアドレスリストは、*定義とユーザ* > *ネットワーク定義* > *MACアドレス定義*タブで定義されます。

4. ***保存*をクリックします。**
新しいルールが*ルール*リストに表示されます。

ファイアウォールルールを有効にします。

5. 新しいルールはデフォルトで無効になっています(トグルスイッチはグレー表示)。ルールを有効にするには、トグルスイッチをクリックします。
これでルールが有効になります(トグルスイッチは緑色)。

ルールを編集または削除するには、対応するボタンをクリックします。

ライブログを開く: フィルタされたパケットのリアルタイムログを含むポップアップウィンドウを開きます。表示は定期的に更新されて、最新のネットワークアクティビティが示されます。適用されたアクションによって、背景色が次のように変化します。

- 赤色:パケットは破棄されました。
- 黄色:パケットは拒否されました。
- 緑色:パケットは許可されました。
- 灰色:アクションを決定できませんでした。

ライブログには、パケットが拒否される原因となったファイアウォールルールに関する情報も含まれます。こうした情報は、ルールのデバッグに必須です。検索機能を使用して、特定のエントリについてファイアウォールログをフィルタすることができます。検索機能では、表現の前にダッシュ(–)を付けることで、その表現を無効にできます。たとえば、`-WebAdmin`と指定すると、この表現を含むすべての行を連続して非表示にできます。

*自動スクロール*チェックボックスにチェックを入れると、ウィンドウのスクロールバーが自動的にスクロールダウンして、常に最新の結果が表示されます。

以下に、ファイアウォールの設定に関する基本的なヒントをいくつか示します。

- ドロップされたブロードキャスト: デフォルトでは、すべてのブロードキャストはドロップされ、ログもされません(詳細は詳細を参照)。この機能はNetBIOS(たとえば、Microsoft Windowsオペレーティングシステム)を使用する多数のコンピュータから成るネットワークで役立ちます。この理由は、ファイアウォールのログファイルは、ブロードキャストによってすぐにいっぱいになるからです。ブロードキャストのドロップルールを手動で定義するには、接続されたすべてのネットワークのブロードキャストアドレスの定義をグループ化し、`255.255.255.255/255.255.255.255`の「global_broadcast」定義を追加し、次にファイアウォール設定上部でこれらのアドレスに対するすべてのトラフィックをドロップするルールを

追加します。ブロードキャストを多用するネットワークでは、これによってシステムのパフォーマンスも向上します。

- **IDENT** トラフィックの リジェクト: IDENTリバースプロキシを使用しない場合は、内部ネットワークのポート`113`(IDENT)へのトラフィックをアクティブに拒否できます。これにより、FTP、IRC、およびSMTPなどのIDENTを使用するサービスの長いタイムアウトを防止できます。

> 注 – マスカレーディングを使用している場合は、マスカレードされているネットワークに対するIDENT要求が、マスカレードするインタフェースに届きます。

- NATはネットワークパケットのアドレスを変更するため、ファイアウォールの機能に影響を与えます。
  - DNATはファイアウォールの*前に*適用します。これは、ファイアウォールが、すでに変換されたパケットを「見る」ことを意味します。DNAT関連のサービスにルールを追加する際は、これを考慮することが必要です。
  - SNATおよびマスカレーディングはファイアウォールの*後に*適用されます。これは、ファイアウォールは、オリジナルの送信元アドレスを持つ変換されていないパケットをまだ「見る」ことを意味します。

テーブルヘッダのコントロールパネルを使用して、特定の基準でファイアウォールルールをフィルタして、読みやすいようにルールを再構成できます。グループを定義している場合は、ドロップダウンメニューからグループを選択し、このグループに属するすべてのルールを見ることができます。検索フィールドを使用して、キーワードあるいは単に文字列を探して、それに関連するルールを表示できます。検索は、ルールの送信元、宛先、サービス、グループ名、およびコメントで構成されます。

8.1.2 送受信国別ブロック

*ネットワークプロテクション > ファイアウォール > 送受信国別ブロック*タブで、特定国からの、または特定国へのトラフィックをブロックできます。1つの国/場所あるいは大陸全体をブロックできます。このブロックは、ホストのIPアドレスのGeoIP情報に基づいています。

送受信国別ブロックを有効にするには、以下の手順に従います。

1. **送受信国別ブロックを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、*国*エリアが編集可能になります。

2. **ブロックする場所を選択します。**

場所名の前にあるドロップダウンリストを使用して、それぞれの場所のブロック状況を指定します:

- *すべて*: この場所へのすべての受信、またはこの場所からのすべての送信がブロックされます。
- *送信元*: この場所を送信元とするトラフィックがブロックされます。
- *宛先*: この場所を宛先とするトラフィックがブロックされます。
- *オフ*: この場所からのトラフィック、ならびにこの場所へのトラフィックが許可されます。

> ヒント – ある地域のすべての場所について、同一のブロックステータスを簡単に選択することができます。これを行うには、それぞれの地域の名前の前にあるドロップダウンリストでブロックステータスを選択します。

3. ***適用*をクリックします。**
   設定が保存されます。

   トグルスイッチが緑に変わり、お使いの設定に従い、選択したロケーションからの/へのトラフィックがブロックされます。*国ブロックの例外*タブで、ブロックされる場所に対して例外を定義することができます。

> ヒント – このページの各セクションは、セクションヘッダの右にあるアイコンをクリックして、折りたたみ/展開できます。

8.1.3 国ブロックの例外

*ネットワークプロテクション > ファイアウォール > 国ブロックの例外*タブでは、*国ブロック*タブでブロックされる国の例外を定義できます。例外は、トラフィックの方向やサービスを考慮に入れて、ブロックされている国/場所と特定のホストまたはネットワークとの間でのトラフィックに適用されます。

国ブロックの例外を作成するには、次の手順に従います。

1. ***新規例外リスト*をクリックします。**
   *除外リストを追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前: 除外を説明する名前を入力します。

   コメント(オプション): 説明などの情報を追加します。

これらのブロックをスキップ:

- 地域 : このドロップダウンリストを使用して、*国*ボックスに表示される国を絞り込むことができます。
- 国 : 例外を指定する国や地域の前にあるチェックボックスを選択します。すべての国を一度に選択するには、*すべてを選択*チェックボックスを有効にします。

> 注 – 例えば内部IPアドレスなど、任意の国に関連していないものも含め、すべてのIPアドレスを選択するには、*すべて外す*チェックボックスを使用し、すべてのチェックボックスからチェックを外します。

全リクエストに適用 : 国ブロックをスキップ条件を選択します。下のボックスで選択したホスト/ネットワークを参照することで、送信および受信を選ぶことができます。

- ホスト/ネットワーク: 上のドロップダウンリストで選択したエントリに応じて、選択した国との送信トラフィックまたは受信トラフィックを許可するホスト/ネットワークを追加または選択します。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

サービスを利用 : オプションで、選択したホスト/ネットワークと選択した国/場所の間で許可するサービスを追加します。サービスが選択されていない場合、すべてのサービスが許可されます。

3. ***保存*をクリックします。**
   新しい国ブロックの例外が*国ブロックの例外*リストに表示されます。

除外ルールを編集または削除するには、対応するボタンをクリックします。

国ブロックの例外を使用する

国ブロックの例外は以下のように使用します:

インタフェース/リモートホスト	要求	ホスト/ネットワーク	国
ローカルインタフェース	送信元	ローカルインタフェースアドレスを入力	スキップする国を選択
ローカルインタフェース	宛先	ローカルインタフェースアドレスを入力	スキップする国を選択
リモートホスト 内部ネットワーク	送信元	内部ホスト/ネットワークを入力	スキップする国を選択

インタフェース/リモートホスト	要求	ホスト/ネットワーク	国
リモートホスト 外部ネットワーク	送信元	外部ホストを入力	国を選択しないでください
リモートホスト 内部ネットワーク	宛先	内部ホスト/ネットワークを入力	スキップする国を選択
リモートホスト 外部ネットワーク	宛先	外部ホストを入力	国を選択しないでください

8.1.4 ICMP

ネットワークプロテクション > *ファイアウォール* > ***ICMP*タブ**で、*インターネット制御メッセージプロトコル*(ICMP)の設定を構成できます。ICMPを使用して、ホスト間で接続関連のステータス情報をやり取りします。ICMPはネットワーク接続のテストやネットワークの問題のトラブルシューティングに重要です。

このタブで任意のICMPトラフィックを許可すると、ファイアウォールのICMP設定が上書きされます。特定のホストやネットワークだけにICMPを許可する場合は、*ファイアウォール* > *ルール*タブを使用します。

グローバルICMP設定

以下のグローバルICMPオプションを利用できます。

- **ゲートウェイ上でのICMPを許可**:このオプションで、どの種類のICMPパケットにもゲートウェイが対応できるようにします。
- **ICMPのゲートウェイ通過を許可**:このオプションを使用すると、内部ネットワーク、つまりデフォルトゲートウェイを使用しないネットワークからパケットが送信される場合、ゲートウェイを通してICMPパケットを転送可能になります。
- **ICMPリダイレクトをログ**:ICMPリダイレクトは、パケットの宛先へのより良いルートを探すために、1台のルータから別のルータに送信されます。ルータはルーティングテーブルを変更して、より適切と想定されるルートを経由して同じ宛先にパケットを送ります。このオプションを選択すると、ゲートウェイが受信したすべてのICMPリダイレクトがファイアウォールログにログされます。

注 – 有効にすると、ICMP設定は、すべてのICMP パケットに適用されます。ICMP経由で送信される場合は、たとえ対応するpingやtracerouteの設定が無効であっても、pingやtracerouteも含まれます。

Ping設定

*ping*プログラムは、IPネットワークを横断して特定ホストに到達できるかどうかをテストするためのコンピュータネットワークツールです。ping は、ICMP *エコー要求*パケットをターゲットホストに送信し、ICMP *エコー応答*による返信を待機することで機能します。ping は、間隔のタイミングと応答率を使用して、ホスト間の往復時間とパケット紛失率を評価します。

以下のpingオプションを利用できます。

- ゲートウェイは**ping**で可視 : ゲートウェイはICMP *エコー要求*パケットに応答します。この機能はデフォルトで有効になっています。
- ゲートウェイからの**ping** : ゲートウェイでpingコマンドを使用できます。この機能はデフォルトで有効になっています。
- ゲートウェイは**ping**を転送 : ゲートウェイは、内部ネットワーク、つまりデフォルトゲートウェイを使用しないネットワークから送信されるICMP *エコー要求* *および*エコー応答パケットを転送します。

注 – 有効であれば、たとえ対応するtracerouteの設定が無効であっても、pingの設定もtraceroute ICMPパケットを許可します。

Traceroute設定

traceroute(トレースルート)プログラムは、IPネットワーク上でパケットが使用するルートの決定に使用されるコンピュータネットワークツールです。tracerouteは、パケットの伝送に関与したルータのIPアドレスを一覧表示します。一定の時間内にパケットのルートを判断できない場合は、IPアドレスの代わりにアスタリスク(*)で報告します。一定の回数だけ失敗すると、確認作業は終了します。確認の中断には多くの理由が考えられますが、ほとんどの場合は、ネットワークパスのファイアウォールが traceroute パケットをブロックすることが原因となります。

以下のtracerouteオプションを利用できます。

- ゲートウェイは**traceroute**で可視 : ゲートウェイはtraceroute パケットに応答します。
- ゲートウェイは**traceroute**を転送 : ゲートウェイは内部ネットワーク、つまりデフォルトゲートウェイを使用しないネットワークから送信されるtracerouteを転送します。

注 – UTM内のブリッジモードではパケットフィルタを使用して、トラフィックがUTMを通過できるようにします(webサーフィントラフィックなど)。この場合、*ICMPのゲートウェイ通過を許可*、*ゲートウェイはpingを転送*、および*ゲートウェイは転送*の各オプションは、ブリッジモードでは機能しなくなります。

注 – さらに、UNIX tracerouteアプリケーション用のUDPポートも開きます。

注 – 有効であれば、たとえ対応するpingの設定が無効であっても、tracerouteの設定もpingパケットを許可します。

8.1.5 詳細

ネットワークプロテクション > *ファイアウォール* > *詳細*タブには、ファイアウォールおよびNATルールの詳細設定が含まれています。

コネクショントラッキングヘルパ

コネクショントラッキングヘルパを使用することにより、複数のネットワークコネクションを使用するプロトコルでファイアウォールあるいはNATルールを使用できます。ファイアウォールが取り扱うすべての接続は、*conntrack*カーネルモジュール(*コネクショントラッキング*プロセスとも呼ばれます)で追跡します。FTPやIRCなどのプロトコルにはいくつかのポートを開くことが必要で、それらの正常な機能をサポートする特別なコネクショントラッキングヘルパが必要になります。これらのヘルパは特別なカーネルモジュールで、追加のコネクションを最初のコネクションに関連付けることによって(通常はデータストリームから関連するアドレスを読み取ることで)特定します。

たとえば、FTPのコネクションが正常に機能するには、FTP conntrackヘルパを選択する必要があります。これはFTPプロトコルの特異性によるもので、それによってFTPコントロールコネクションと呼ばれる単一のコネクションを確立します。このコネクションでコマンドが発行されると、他のポートが開いてその特定コマンドに関連するデータの残りを実行します(例:ダウンロードあるいはアップロード)。問題は、それらは動的にネゴシエートされたため、ゲートウェイがこれらの特別なポートを知らない、ということです。したがって、ゲートウェイは、これらの特定のポートでサーバをクライアントに接続させなければならないか(アクティブなFTP接続)、またはインターネット上でクライアントをFTPサーバに接続させなければならないか(パッシブなFTP接続)を知ることができません。

これがFTP conntrackヘルパが役に立つ理由です。この特別なヘルパは特別なコネクショントラッキングモジュールに追加され、特別な情報のコントロールコネクション(通常はポート21)をスキャンします。ヘルパが正しい情報に出会うと、その情報をコントロールコネクションの関連情報として想

定される接続のリストに追加します。これにより、ゲートウェイで最初のFTPコネクションと関連する全コネクションの両方を追跡することが可能になります。

コネクショントラッキングヘルパは以下のプロトコルで使用できます。

- FTP
- IRC（DCC用）
- PPTP
- TFTP

注 - ファイアウォールでPPTP VPNサービスを提供したい場合は、PPTPヘルパモジュールをロードする必要があります。ロードしないと、PPTPセッションは確立できません。この理由は、PPTPは、別個のIPプロトコルの*Generic Routing Encapsulation*（GRE）通信に切り換える前に、TCPポート1723接続を確立するからです。PPTPヘルパモジュールをロードしないと、すべてのGREパケットはゲートウェイにブロックされます。PPTPヘルパモジュールを使用しない場合は、代わりにファイアウォールルールを手動で追加し、受信および送信トラフィックでGREパケットを許可します。

プロトコル処理

TCPウインドウスケーリングの有効化：TCPの受信ウインドウ（RWin）サイズは、接続時にバッファできる受信データ量（バイト単位）です。送信側ホストは、受信側ホストからの受信確認とウィンドウの更新を待つ間、その量のデータのみを送信できます。高帯域幅ネットワークをさらに効率的に使用するために、大きなTCPウインドウサイズを使用できます。ただし、TCPウインドウサイズのフィールドはデータの流れを制御し、2バイトあるいは65535バイトのウインドウサイズに制限されています。サイズフィールドは拡張できないため、スケーリングファクタを使用します。TCPウインドウのスケーリングはTCP/IPスタックのカーネルオプションで、最大ウインドウサイズを65535バイトから1ギガバイトに拡大するために使用できます。デフォルトではウインドウスケーリングが有効になっています。しかし、ルータ、ロードバランサ、ゲートウェイなどの一部のネットワークデバイスはウインドウのスケーリングをまだ完全にはサポートしていないため、環境によってはスケーリングをオフにすることが必要な場合があります。

厳密なTCPセッション処理を使用する：デフォルトでは、システムはネットワーク機能のリセットによりコネクショントラッキングテーブルで現在扱われていない既存のTCPコネクションを「ピックアップ」できます。これはSSHおよびTelnetなどの対話型セッションが、ネットワークインタフェースが一時的に利用できない場合に停止しないことを意味します。このオプションを有効にすると、そのようなセッションを再度確立するには新しい3WAYハンドシェークが常に必要になります。さらに、このオプションはTCP接続方法が同時に開くことや、TCPがハンドシェークを分割することを許可しません。一般的にはこのオプションはオフのままにしておくことをお勧めしています。

パケット長の有効性を確認：有効にすると、ファイアウォールは、ICMP、TCP、またはUDPプロトコルの使用時に、データパケットが最小長を満たしているかチェックします。データパケットが最小値より小さい場合、それらはブロックされ、その記録がファイアウォールログに書き込まれます。

なりすまし防御：デフォルトでは、なりすまし防御は無効になっています。以下の設定から選択できます。

- 通常：ゲートウェイは、インタフェース自体と同じ送信元IPアドレスを持つパケット、またはそのインタフェースに別に割り当てられたネットワークの送信元IPを持つインタフェースに到着するパケットを、ドロップしてログします。
- 厳密：ゲートウェイは、宛先IPにインタフェースが指定され、割り当てられた以外のインタフェースに到着する（つまり、宛先として指定されていないインタフェースに到着する）すべてのパケットを、ドロップしてログします。たとえば、内部ネットワークのみからパケットを受け付けると想定される内部インタフェースのIPアドレスに外部ネットワークから送信されたパケットはドロップされます。

ロギングオプション

***FTP**データコネクションのログ*：UTMは、ファイルおよびディレクトリリスティングのFTPデータコネクションをログします。ログレコードには「FTP data（FTPデータ）」という文字列によってマークが付けられます。

*ユニークな**DNS**リクエストのログする*：UTMは、DNSサーバへのすべての要求およびそれらの結果をログします。ログレコードには「DNS request」という文字列によってマークが付けられます。

破棄したブロードキャストのログ：デフォルトでは、ファイアウォールはすべてのブロードキャストを破棄し、ログも行いません。しかし、たとえば監査のためにブロードキャストをファイアウォールログに記録する必要がある場合は、このオプションを選択します。

8.2 NAT

*ネットワークプロテクション > NAT*メニューを使用すると、ゲートウェイのNATルールを定義し、管理することができます。*ネットワークアドレス変換*（NAT）とは、ルータやゲートウェイを通過するIPパケットの送信元アドレスまたは宛先アドレス（あるいは両方）を書き換えるプロセスです。NATを使用するほとんどのシステムは、プライベートネットワーク上の複数のホストが1つのパブリックIPアドレスを使用してインターネットにアクセスできるようにするためにNATを使用しています。あるクライアントがIPパケットをルータに送信すると、NATは送信アドレスを別のパブリックIPアドレスに変換してからインターネットにパケットを転送します。応答パケットを受信すると、NATはパブリックアドレスを元のアドレスに変換し、クライアントにパケットを転送します。システムリソースに応じて、NATは自己裁量で大規模内部ネットワークに対応できます。

8.2.1 マスカレード

マスカレードとは、*送信元ネットワークアドレス変換*（SNAT）の特殊ケースであり、ネットワークインタフェース（通常は、インターネットに接続された外部インタフェース）上の 1つの公式 IP アドレスの背後に内部ネットワーク（通常はプライベートアドレススペースを持つ LAN）をマスカレードすることができます。SNATの場合、複数の送信元アドレスを複数の宛先アドレスにマッピングすることができるため、より汎用的です。

注 – 送信元アドレスは、指定されたインタフェース経由でパケットがゲートウェイシステムから配信された場合にのみ変換されます。新しい送信元アドレスは常に、当該インタフェースの最新IPアドレスとなります（つまり、このアドレスは動的です）。

マスカレードルールを作成するには、次の手順に従います。

1. ***マスカレード*タブで*新規マスカレードルール*をクリックします。**
   *マスカレードルールの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   ネットワーク：マスカレードする（内部）ネットワークを選択します。

   優先順位：ルールの優先順位を定義する位置番号。番号が小さいほど優先順位が高くなります。ルールは昇順に照合されます。あるルールが一致すると、それ以降、それより大きい番号のルールは評価されません。

   インタフェース I/F ：インターネットに接続する（外部）インタフェースを選択します。

   アドレスを使用：選択したインタフェースに複数のIPアドレスが割り当てられている場合（*インタフェースとルーティング > 追加アドレス*参照）、マスカレードに使用するIPアドレスをここで定義できます。

   コメント（オプション）：説明などの情報を追加します。

3. ***保存*をクリックします。**
   新しいマスカレードルールが*マスカレード*ルールのリストに表示されます。

4. **マスカレードルールを有効にします。**
   マスカレードルールを有効にするには、トグルスイッチをクリックします。

ルールを編集または削除するには、対応するボタンをクリックします。

> 注 – クライアントが外部サーバにアクセスできるようにするには、ファイアウォールで内部ネットワークからインターネットへのトラフィックを許可する必要があります。

IPsecパケットはマスカレードルールの影響を受けません。IPsecパケットの送信元アドレスを変換するには、SNATまたはフルNATルールを作成します。

8.2.2 NAT

DNAT(Destination Network Address Translation)と*SNAT*(Source Network Address Translation)は、いずれもNATの特殊ケースです。SNATでは、接続を開始したコンピュータのIPアドレスが書き換えられます。一方、DNATでは、データパケットの宛先アドレスが書き換えられます。DNATは、内部ネットワークでプライベートIPアドレスを使用しており、管理者が一部のサービスを外部からも使用可能にしたい場合に特に便利です。

これは、例を使って説明するとわかりやすいでしょう。内部ネットワークでアドレススペース`192.168.0.0/255.255.255.0`を使用しており、WebサーバがIPアドレス`192.168.0.20`で機能しているとします。この場合、インターネット経由のクライアントに対してポート`80`を使用可能にする必要があります。`192.168.`アドレススペースはプライベートであるため、インターネットベースのクライアントはWebサーバにパケットを直接送信できません。ただし、UTMの外部(公開)アドレスと通信することはできます。この場合、DNATは、システムアドレスのポート`80`向けのパケットを捕捉し、内部Webサーバに転送できます。

> 注 – *PPTP VPN アクセス*はDNATに対応していません。

常にプライマリネットワークインタフェースアドレスにマッピングするマスカレードと異なり、SNATは送信元アドレスをSNATルールに指定されたアドレスにマッピングします。

1:1 NATはDNATまたはSNATの特殊なケースです。この場合、ネットワーク全体のすべてのアドレスが同じネットマスクを持つ別のネットワークのアドレスに1対1で変換されます。したがって、元のネットワークの最初のアドレスが他のネットワークの最初のアドレスに変換され、元のネットワークの2番目のアドレスが他のネットワークの2番目のアドレスに変換されるという様になります。1:1のNATルールは、送信元アドレスまたは宛先アドレスに適用することができます。

> 注 – デフォルトで、ポート`443`(HTTPS)はユーザポータルに使用されます。ポート`443`を内部サーバに転送する予定がある場合、*マネジメント* > *ユーザポータル* > *詳細*タブでユーザポータルのTCPポートを他の値(`1443`など)に変更する必要があります。

DNATはファイアウォールの前に行われるため、適切なファイアウォールルールを定義しておく必要があります。詳しくは、*ネットワークプロテクション* > *ファイアウォール* > *ルール*を参照してください。

NATルールを定義するには、次の手順に従います。

1. ***NAT*タブで、*新規NATルール*をクリックします。**
   *NATルールの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   グループ: *グループ*オプションを使用すると、ルールを論理的にグループ化できます。リストの上部にあるドロップダウンリストを使用すると、ルールをグループ別にフィルタできます。グループ化は表示用のみで、ルールの一致には関係ありません。新しいグループを作成するには、<<*新規グループ*>>エントリを選択し、グループを説明する名前を*名前*に入力します。

   優先順位: ルールの優先順位を定義する位置番号。番号が小さいほど優先順位が高くなります。ルールは昇順に照合されます。あるルールが一致すると、それ以降、それより大きい番号のルールは評価されません。

   ルールタイプ: ネットワークアドレス変換モードを選択します。選択に応じて、さまざまなオプションが表示されます。次のモードを使用できます。

   - **SNAT** 送信元 : 定義されたIPパケットの送信元アドレスを1つの新しい送信元アドレスにマッピングします。サービスを変更することもできます。

   - **DNAT** 宛先 : 定義されたIPパケットの宛先アドレスを1つの新しい宛先アドレスにマッピングします。サービスを変更することもできます。

   - **1:1 NAT** ネットワーク全体 : ネットワークのIPアドレスを別のネットワークに1対1でマッピングします。このルールは、定義されたIPパケットの送信元アドレスか宛先アドレスに適用されます。

   - *フル***NAT** 送信元+宛先 : 定義されたIPパケットの送信元アドレスと宛先アドレスの両方を1つの新しい送信元アドレスと1つの新しい宛先アドレスにマッピングします。送信元サービスとターゲットサービスを変更することもできます。

   - **NAT**除外 : このオプションは除外ルールの一種と考えることができます。たとえば、定義したネットワークにNATルールがある場合、このネットワーク内の特定のホストに対して*NAT除外*ルールを作成することができます。これにより、これらのホストはNATの対象外となります。

   *マッチング*条件 : 送信元および宛先ネットワーク/ホストとアドレスを変換するサービスを追加または選択します。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

- *トラフィック送信元*：パケットのオリジナルの送信元アドレス。1つのホストにすることも、ネットワーク全体にすることもできますし、*1:1 NAT*ルールタイプを除けば、ネットワーク範囲にすることもできます。
- *サービス*：パケットのオリジナルのサービスタイプ（送信元ポートと宛先ポート、およびプロトコルタイプから構成されています）。

> 注 – トラフィックサービスは、対応するアドレスも変換される場合のみ変換できます。さらに、2つのサービスが同じプロトコルが使用する場合のみ、サービスを別のサービスに変換できます。

- *トラフィック宛先*：パケットのオリジナルの宛先アドレス。1つのホストにすることも、ネットワーク全体にすることもできます。*SNAT* および*NAT なし*では、ネットワーク範囲にすることもできます。

アクション：送信元/宛先、元のIPパケットデータを変換するサービスタイプを追加または選択します。表示されるパラメータは選択されている*ルールタイプ*に依存します。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

- 変更後の送信元（*SNAT*または*フルNAT*モードのみ）：送信元ホスト、つまりパケットの新しい送信元アドレスを選択します。
- 変更後の宛先（*DNAT*または*フルNAT*モードのみ）：宛先ホスト、つまりパケットの新しい宛先アドレスを選択します。
- 変更後のサービス（*DNAT*、*SNAT*、または*フルNAT*モードのみ）：パケットの新しいサービスを選択します。選択されている*ルールタイプ*によっては、送信元/宛先サービスとすることができます。
- **1:1 NAT** モード（*1:1 NAT*ルールタイプのみ）：以下のモードのいずれかを選択します。
  - 宛先のマッピング：宛先アドレスを変更します。
  - 送信元のマッピング：送信元アドレスを変更します。

> 注 – 送信元をマッピングする場合は、*トラフィック送信元*フィールドにネットワーク全体を追加し、宛先をマッピングする場合は*トラフィック宛先*フィールドにネットワーク全体を追加する必要があります。

- マッピング先(*1:1 NAT*モードのみ):元のIPアドレスの変換先となるネットワークを選択します。元のネットワークと変換先のネットワークが同じネットマスクである必要があります。

自動ファイアウォールルール(オプション):該当するトラフィックがファイアウォールを通過することを許可するファイアウォールルールを自動的に生成する場合に、このオプションを選択します。

コメント(オプション):説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**
   IPsecパケットにルールを適用(*SNAT*または*フルNAT*モードのみ):IPsecで処理するトラフィックにルールを適用する場合にこのオプションを選択します。デフォルトではこのオプションが選択されていないため、IPsecトラフィックがSNATから除外されることになります。

   初期パケットのログ(オプション):このオプションは、通信の初期化パケットをファイアウォールログに書き込む場合に選択します。これにより、NATルールを使用する場合はいつでも、ファイアウォールログに「NATを使用する接続」というメッセージが記述されます。このオプションは、ステートフルプロトコルでもステートレスプロトコルでも機能します。

4. *保存*を**クリックします。**
   新しいルールが*NAT*リストに表示されます。

   NATルールを有効にします。

5. 新しいルールはデフォルトで無効になっています(トグルスイッチはグレー表示)。ルールを有効にするには、トグルスイッチをクリックします。

ルールを編集または削除するには、対応するボタンをクリックします。

8.3 高度な脅威防御

*ネットワークプロテクション > 高度な脅威防御(ATP)*メニューで、高度な脅威防御機能を有効にし、設定することで、ネットワーク内の感染した、または使用できなくなったクライアントを速やかに検出し、それぞれのトラフィックについて、アラートを発生させるか、ドロップさせることができます。高度な脅威防御は、現在の企業ネットワークにおける一般的な課題を対象としています:一方では、さまざまなモバイルデバイスの台数が増加する中でのモバイル従業員の管理(BYOD)であり、もう一方は、ますます高速化しつつあるマルウェアの進化や拡散の方法です。高度な脅威防御は、ネットワークのトラフィックを分析します。たとえば、DNSリクエスト、HTTPリクエスト、あるいは、一般に、すべてのネットワークとの間でやり取りされるIPパケットなどです。また、それぞれの機能が有効であれば、侵入防御やウイルス対策のデータも取り込みます。脅威を特定するために使用されるデータベースは、パターンの更新を通じてSophos LabsからフィードされるCnC/Botnet

データによって継続的に更新されます。このデータに基づいて、感染したホストや、そのコマンド・アンド・コントロール（CnC）サーバとの通信が、速やかに特定され、対処されます。

8.3.1 グローバル

高度な脅威防御(ATP) > *グローバル*タブで、Sophos UTMの*高度な脅威防御システム*を有効にすることができます。

高度な脅威防御を有効にするには、以下の手順に従います。

1. **高度な脅威防御システムを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、*グローバル設定*エリアが編集可能になります。

2. **次の設定を行います。**
   ポリシ: 脅威が検出された場合に高度な脅威防御システムが使用するべきセキュリティポリシを選択します。

   - 破棄: データパケットは記録され、ドロップされます。
   - 警告: データパケットは記録されます。

   ネットワーク/ホスト除外:高度な脅威防御による脅威のスキャンから除外されるべき、送信元ネットワークまたはホストを追加または選択します。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

   脅威除外:高度な脅威防御による脅威のスキャンでスキップしたい宛先IPアドレスまたはドメイン名を追加します。これは、脅威として検出されることを防ぐために、誤検出を追加するべき場所です。例:`8.8.8.8`または`google.com`。

   > 警告 – 除外の指定には、注意してください。送信元や宛先を除外することで、ネットワークをより深刻なリスクに曝すことになる場合があります。

3. ***適用*をクリックします。**
   設定が保存されます。

   トグルスイッチが緑色に変わります。

有効になっていて、脅威が検出されると、ネットワークプロテクションページにリストされます。*マネジメント* > *通知* > *通知*ページで有効になっていると、通知が管理者に送信されます。通知は、ドロップおよびアラート用にデフォルトで設定されています。

ライブログ

高度な脅威防御のライブログは、検出した脅威のモニタリングに使用できます。ボタンをクリックして、新しいウィンドウでライブログを開きます。

注 – IPSおよびWebプロキシの脅威は、*ライブログ*には表示されません。

8.4 侵入防御(IPS)

ネットワークプロテクション > *侵入防御(IPS)*メニューで、ゲートウェイのIPSルールを定義し、管理することができます。侵入防御システム(IPS)は、シグニチャに基づく*IPS*ルールセットを利用して攻撃を認識します。システムは、トラフィックを完全に分析し、ネットワークに到達する前に攻撃を自動的にブロックします。既存のルールセットと攻撃パターンは、パターン更新によって最新状態に更新されます。IPS攻撃パターンのシグニチャは、IPSルールとしてルールセットに自動的にインポートされます。

8.4.1 グローバル

ネットワークプロテクション > *侵入防御(IPS)* > *グローバル*タブでは、Sophos UTMの*侵入防御システム*(IPS)を有効にすることができます。

IPSを有効にするには、次の手順に従います。

1. **侵入防御システムを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、*グローバルIPS設定*エリアが編集可能になります。

2. **次の設定を行います。**
   ローカルネットワーク: 侵入防御システムで防御するネットワークを追加または選択します。ローカルネットワークを選択しないと、侵入防御は自動的に無効になり、トラフィックはモニタリングされません。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

   ポリシ: ブロッキングルールがIPS攻撃シグニチャを検出したときに侵入防御システムが使用するセキュリティポリシを選択します。

- サイレントドロップ:データパケットは、他のアクションなしでドロップされます。
- コネクションを切断:中止データパケット(TCPの場合は*RST*、UDPコネクションの場合は*ICMP Port Unreachable*)が両方の通信相手一に送信され、コネクションがクローズされます。

注 – デフォルトでは、*サイレントドロップ*が選択されています。通常はこの設定を変更する必要はありません。これは特に、疑わしい侵入者に中止データパケットが悪用され、ゲートウェイについての情報が引き出されてしまう可能性があるためです。

3. ***適用*をクリックします。**
   設定が保存されます。

   トグルスイッチが緑色に変わります。

ライブログ

侵入防御ライブログは、選択したIPSルールのモニタリングに使用できます。ボタンをクリックして、新しいウィンドウでライブログを開きます。

8.4.2 攻撃パターン

*ネットワークプロテクション > 侵入防御 > 攻撃パターン*タブには、共通の攻撃パターンに従ってグループ分けされたIPSルールが表示されます。攻撃パターンは次のようにまとめられています。

- オペレーティングシステム固有の攻撃:オペレーティングシステム関連の脆弱性を悪用しようとする攻撃。
- サーバに対する攻撃:(Webサーバ、メールサーバなど)あらゆる種類のサーバを対象とする攻撃。
- クライアントソフトウェアに対する攻撃:Webブラウザ、マルチメディアプレーヤなどのクライアントソフトウェアを対象とする攻撃。
- プロトコル異常:ネットワークの異常を探す攻撃パターン。
- マルウェア:所有者のインフォームドコンセントなく、コンピュータシステムへの侵入や破壊を行うように設計されたソフトウェア(トロイの木馬、DoS通信ツールなど)。

パフォーマンス向上のために、会社のローカルネットワークに導入されているサービスまたはソフトウェアに該当しないチェックボックスはチェックを外してください。たとえば、ローカルネットワーク内でWebサーバを運用していない場合は、*HTTPサーバ*用の選択を取り消すことができます。

各グループに対して、次の設定を使用できます。

アクション: デフォルトで、グループ内の各ルールにはアクションが関連付けられています。次のアクションを選択できます。

- 破棄: デフォルト設定。攻撃の疑いがある試行が見つかると、その原因であるデータパケットはドロップされます。
- 警告: *破棄*設定と違い、重大なデータパケットはゲートウェイを通過できますが、IPSログにアラートメッセージが記述されます。

注 – 個々のIPSルールの設定を変更するには、*侵入防御* > *詳細*タブの*変更されたルール*ボックスを使用します。Sophos UTM9で使用されているIPSルールの詳細なリストは、UTM Web サイトで参照できます。

ルールの有効期間: デフォルトでは、IPSパターンの有効期間は12か月です。全体的なパッチレベル、レガシーシステム、その他のセキュリティ要件などの個々の要因によって、他の期間を選択することもできます。短い期間を選択すると、ルールの数を減少できるため、パフォーマンスも向上できます。

追加の警告ルールを有効化: このオプションを選択すると、各グループにルールが追加され、IPS検出率が向上します。これらのルールは、明示的な攻撃パターンよりも一般的で曖昧なので、アラートの数が増える可能性があります。このため、これらのルールのデフォルトアクションは*警告*であり、設定はできません。

通知: このオプションを選択すると、このグループと一致するIPSイベントが発生するたびに管理者に通知が送信されます。このオプションが有効になるのは、*マネジメント* > *通知* > *通知*タブで侵入防御システムの通知機能を有効にした場合のみです。さらに、送信される通知のタイプ(つまり、EメールまたはSNMPトラップ)は、ここでの設定によって決まります。また、通知設定の変更が有効になるまでは最大5分かかる場合があります。

8.4.3 DoS/フラッド防御

*DoS/フラッド防御*タブでは、DoS *サービス拒否* 攻撃とDDoS *分散型サービス拒否* 攻撃から防御するためのオプションを設定できます。

一般にDoS攻撃とDDoS攻撃は、正当な要求がコンピュータリソースを使用できないようにします。シンプルな例では、攻撃者はサーバに無意味なパケットを送信して過負荷をかけ、パフォーマンスに負担をかけます。このような攻撃には大規模な帯域幅が必要となるため、いわゆる*SYN フラッド攻撃*を使用する攻撃者が増え続けています。この攻撃は、帯域幅の過負荷ではなく、システムリソースのブロックを目的としています。この目的のために、攻撃者は多くの場合、偽造された送信元アドレスを使用してサービスのTCPポートにSYNパケットを送信します。これに対し、サーバは

TCP/SYN-ACKを送り返して、これに応答する送信元アドレスからのTCP/ACKパケットを待ち続けるため、接続がhalf-open状態になります。ところが、送信元アドレスは偽造されているため、応答は返ってきません。これらのhalf-open状態の接続により、サーバが対応できる接続数が飽和状態になり、正当な要求に対応できなくなります。

このような攻撃は、特定時間内にネットワークに対して送信されるSYN(TCP)、UDP、ICMPパケットの数を制限することで回避できます。

TCP SYNフラッド防御

SYN(TCP)フラッド防御を有効にするには、次の手順に従います。

1. ***DoS/フラッド防御*タブで、*TCP SYNフラッド防御の使用*チェックボックスにチェックを入れます。**

2. **次の設定を行います。**
   モード: 次のモードを使用できます。

   - *送信元アドレスと宛先アドレス*: 送信元IPアドレスと宛先IPアドレスの両方によってSYNパケットをドロップする場合、このオプションを選択します。まず、送信元IPアドレスと一致するSYNパケットが、下で指定する送信元パケットレートの値に制限されます。次に、要求がまだ多すぎる場合には、宛先IPアドレスに従って追加でフィルタされ、下で指定する宛先パケットレートの値に制限されます。このモードはデフォルトで設定されています。

   - *宛先アドレスのみ*: 宛先IPアドレスおよび宛先パケットレートのみに従ってSYNパケットをドロップする場合、このオプションを選択します。

   - *送信元アドレスのみ*: 送信元IPアドレスおよび送信元パケットレートのみに従ってSYNパケットをドロップする場合、このオプションを選択します。

   ログ: このオプションを使用すると、ログレベルを選択できます。以下のレベルを設定できます。

   - *オフ*: ログを完全にオフにする場合、このログレベルを選択します。

   - *制限*: ログを1秒あたり5パケットに制限する場合、このログレベルを選択します。デフォルトではこのレベルが設定されています。

   - *すべて*: すべてのSYN(TCP)接続試行を詳細にログする場合、このログレベルを選択します。SYN(TCP)フラッド攻撃により、ログが膨大になる可能性があります。

   送信元パケットレート: ここに、送信元IPアドレスに対して許可される1秒あたりのパケットレートを指定できます。

宛先パケットレート: ここに、宛先IPアドレスに対して許可される1秒あたりのパケットレートを指定できます。

> 注 – ここで合理的な値を入力することは重要です。レートを高く設定し過ぎると、Webサーバがそのように大量なSYN(TCP)パケットに対処しきれず、障害が発生する可能性などがあります。一方、レートを低く設定し過ぎると、ゲートウェイが通常のSYN(TCP)要求をブロックして、予期しない挙動をする可能性があります。各システムの合理的な設定は、ハードウェアに大きく依存します。従って、システムに適した値にデフォルト値を置き換えてください。

3. ***適用*をクリックします。**
   設定が保存されます。

UDPフラッド防御

*UDPフラッド防御*機能は、UDPパケットフラッドを検出し、ブロックします。*UDPフラッド防御*の設定は、*TCP SYNフラッド防御*の設定と同じです。

ICMPフラッド防御

*ICMPフラッド防御*機能は、ICMPパケットフラッドを検出し、ブロックします。*ICMPフラッド防御*の設定は、*TCP SYNフラッド防御*の設定と同じです。

8.4.4 ポートスキャン防御

*ネットワークプロテクション > 侵入防御 > ポートスキャン防御*タブでは、一般的なポートスキャン検知オプションを設定することができます。

ポートスキャンとは、セキュアなシステムで使用可能なサービスを探るためにハッカーが用いる手段です。攻撃者は、システムに侵入したり、DoS攻撃を開始するために、ネットワークサービスに関する情報を必要としています。このような情報を入手すると、攻撃者はこれらのサービスにあるセキュリティ上の欠陥を悪用しようとします。インターネットプロトコルTCPおよびUDPを使用しているネットワークサービスは、特別なポートからアクセス可能であり、このポート割り当ては一般によく知られています。たとえば、SMTPサービスはTCPポート25に割り当てられています。サービスで使用されるポートは、オープンであると見なされます。これは、このようなポートへの接続を確立することができるためです。一方、使用されていないポートはクローズと見なされ、これらのポートへの接続を試みると失敗します。攻撃者は、ポートスキャナという特別なソフトウェアツールを利用してオープンポートを探します。このプログラムは、攻撃対象のコンピュータ上にある複数のポートに対して接続を試みます。接続が成功したポートはオープンであるとツールに表示されます。こうして

攻撃者は、攻撃対象のコンピュータにおいてどのネットワークサービスが使用可能であるかを示す必要な情報を入手します。

インターネットプロトコルTCPとUDPでは、使用可能なポートが全部で65535個あるため、ポートは非常に短い間隔でスキャンされます。サービスへ接続しようとする試行が異常に大量に発生していることをゲートウェイが検出した場合(特に、これらの試行が同じ送信元アドレスから送信されている場合)、ゲートウェイがポートスキャンを受けている可能性が高くなります。攻撃者の疑いのある人がネットワーク上のホストまたはサービスのスキャンを行うと、ポートスキャン検出機能がこれを認識します。オプションで、同じ送信元アドレスから繰り返されるポートスキャンを自動的にブロックすることができます。ポートスキャン検知は、インターネットインタフェース、つまりデフォルトゲートウェイを装備したインタフェースに制限されています。

技術的に言うと、ポートスキャンが検出されるのは、1つの送信元IPアドレスの検出スコアが300ミリ秒の時間枠内で21点を超えたときです。検出スコアは次のように計算されます。

- `1024`未満のTCP宛先ポートに対するスキャン=3点
- `1024`以上のTCP宛先ポートに対するスキャン=1点

ポートスキャン検出を有効するには、次の手順に従ってください。

1. ***ポートスキャン防御*タブで、*ポートスキャン検知*を有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチが緑色になり、*グローバル設定*エリアが編集可能になります。

2. **次の設定を行います。**
   アクション: 次の作業を実行できます。

   - *イベントのログのみ*: ポートスキャンに対する対策は行われません。イベントのログが記録されるだけです。
   - *トラフィックのドロップ*: さらなるポートスキャンパケットは、ユーザに通知することなくドロップされます。ポートスキャナは、これらのポートがフィルタされたことを報告します。
   - *トラフィックの拒否*: さらなるポートスキャンパケットはドロップされ、ICMP「destination unreachable/port unreachable(宛先到達不可/ポート到達不可)」応答が送信者に送られます。ポートスキャナは、これらのポートがクローズされたことを報告します。

   ログを制限: ログメッセージの数を抑えたい場合に、このオプションを有効にします。ポートスキャン検出機能は、ポートスキャンが実行されているときに大量のログを生成します。たとえば、ポートスキャンに使用されていると見なされるそれぞれのSYNパケットに対して、ファイアアウォールログにエントリが1つ生成されます。このオプションを選択すると、ログが1秒あたり5行までに制限されます。

3. *適用*をクリックします。
   設定が保存されます。

8.4.5 除外

*ネットワークプロテクション > 侵入防御 IPS > 除外*タブでは、侵入防御から除外する送信元ネットワークと宛先ネットワークを定義することができます。

注 – 新しいIPS除外は新しい接続にのみ適用されます。新しいIPS除外を既存の接続に適用するには、例えば対応するデバイスを切断するまたは再起動することが可能です。

除外ルールを作成するには、次の手順に従います。

1. **除外タブで、新規除外リストをクリックします。**
   *除外リストを追加*ダイアログボックスが開きます。
2. **次の設定を行います。**
   名前:この除外ルールを説明する名前を入力してください。

   実行しないチェック:スキップするセキュリティチェックを選択します。

   - **侵入防御(IPS)**:このオプションを選択すると、Sophos UTMのIPSが無効になります。
   - ポートスキャン防御:このオプションを選択すると、ネットワークホストでオープンポートを探すことを目的とする攻撃からの防御が無効になります。
   - **TCP SYN**フラッド防御:選択すると、TCPSYNフラッド攻撃からの防御が無効になります。
   - **UDP**フラッド防御:選択すると、UDPフラッド攻撃からの防御が無効になります。
   - **ICMP**フラッド防御:選択すると、ICMPフラッド攻撃からの防御が無効になります。

   対象:セキュリティチェックをスキップする条件を少なくとも1つ選択します。条件の前にあるドロップダウンリストで*And*または*Or*を選択して、複数の条件を論理的に組み合わせることができます。次の条件を設定できます。

   - 送信元ホスト/ネットワークで除外:選択して、この除外ルールのセキュリティチェックから除外する送信元ホスト/ネットワークを追加します。条件を選択すると*ネットワーク*ボックスが開くので、各ホストまたはネットワークを入力します。

- 除外するサービス: 選択して、この除外ルールのセキュリティチェックから除外するサービスを追加します。条件を選択すると*サービス*ボックスが開くので、各サービスを追加します。
- 除外する宛先 : 選択して、この除外ルールのセキュリティチェックから除外するホスト/ネットワークを追加します。条件を選択すると*宛先*ボックスが開くので、各ホストまたはネットワークを入力します。

ヒント – 定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

コメント(オプション) : 説明などの情報を追加します。

3. ***保存*をクリックします。**
   新しい除外ルールが*除外*リストに表示されます。

4. **除外リストを有効にします。**
   新しい例外はデフォルトで無効になっています(トグルスイッチはグレー表示)。例外を有効にするには、トグルスイッチをクリックします。

   これで除外リストが有効になります(トグルスイッチは緑色)。

除外ルールを編集または削除するには、対応するボタンをクリックします。

注 – ゲートウェイの宛先アドレスを持つパケットに対する侵入防御を除外したい場合、*宛先*で*すべて*を選択すると成功しません。そうではなく、例えば*内部 アドレス* または外部WANアドレスなどの、ゲートウェイのIPアドレスを含む宛先を選択します。

注 – UTMプロキシを使用している場合、侵入防御除外がこれを反映している必要があります。プロキシはパケットの元の送信元アドレスをそれ自体のアドレスに置き換えます。したがって、プロキシパケットの侵入防御を除外するには、適切なUTMのインタフェースアドレス定義を送信元*ネットワーク*ボックスに追加する必要があります。

8.4.6 詳細

パターンセットの最適化

ファイル関連パターンを有効にする: デフォルトでは、ファイルに基づく攻撃に対するパターンは、これらの脅威が通常はウイルス対策エンジンによってカバーされているので、保護としては無効になっています。このデフォルトの設定(無効)によって、このオプションが最大の認識率を提供でき

るようにしながら、最大のパフォーマンスを実現しています。他のウイルス保護を使用できない場合、ファイル関連パターンを有効にすることは妥当な選択肢です。つまり、Webプロテクションをオフにするか、クライアントのウイルス対策プログラムをインストールしないことになります。

マニュアルルール変更

このセクションでは、各IPSルールを手動で変更し、攻撃パターングループから取得されるデフォルトポリシを上書きできます。熟練ユーザのみが設定してください。

変更したルールを作成するには、次の手順に従います。

1. *変更されたルール***ボックスで、「+」アイコンをクリックします。**
   *ルールの変更*ダイアログボックスが開きます。

2. **次の設定を行います。**
   ルール**ID**:変更したいルールのIDを入力します。ルールIDを検索するにはSophosのWebサイトでIPSルールのリストにアクセスします。(フォルダで、名前に*IPS-rules*があり、HTMおよびXMの両方のフォーマットで、異なるUTMのバージョンやパターンのバージョンが使用できるファイルを探します。)さらに、IPSログまたはIPSレポートでも決定できます。

   このルールを無効化:このオプションを選択すると、該当IDのルールが無効になります。

   選択*しない*場合、次の2つのオプションを使用できます。

   - 通知の無効化:このオプションを選択すると、当該ルールが適用された場合に通知がトリガされません。
   - *アクション*:各ルールが関連付けられるアクション。次のアクションを選択できます。
     - 破棄:攻撃の疑いがある試行が見つかると、その原因であるデータパケットはドロップされます。
     - 警告:*破棄*設定と違い、重大なデータパケットはゲートウェイを通過できますが、IPSログにアラートメッセージが記述されます。

3. *保存***をクリックします。**
   *変更されたルール*ボックスにルールが表示されます。変更を確定するためには、ページの一番下にある*適用*をクリックする必要もあります。

注 – *変更されたルール*ボックスにルールIDを追加し、アクションを*警告*に設定した場合、この変更が有効になるのは、ルールが属するグループが*攻撃パターン*タブで有効になっている場合のみです。該当する攻撃パターングループが無効になっている場合、各IPSルールへの変更は効果がありません。

パフォーマンスチューニング

さらに、侵入防御システムのパフォーマンスを向上し、誤検出による警告を最低限に抑えるために、IPSルールの範囲を内部サーバの一部に制限することができます。たとえば、*攻撃パターン*タブで*HTTPサーバ*を有効にし、特定のHTTPサーバをここで選択したとします。この場合、侵入防御システムがHTTPサーバへの攻撃を認識しても、関連付けられたアクション(*ドロップ*または*アラート*)は、影響を受けるサーバのIPアドレスとここで選択されたHTTPサーバのIPアドレスが一致する場合に限り、適用されます。

次のサーバタイプに対して、IPSルールの範囲を制限できます。

- **HTTP**: *HTTPサーバ*に含まれるすべての攻撃パターングループ
- **DNS**: 攻撃パターングループ*DNS*
- **SMTP**: 攻撃パターングループ*Exchange*および*Sendmail*
- **SQL**: *データベースサーバ*に含まれるすべての攻撃パターングループ

8.5 サーバロードバランシング

サーバーロードバランシング機能により、受信接続(例: SMTP または HTTPトラフィック)をゲートウェイの背後の複数サーバーに分散できます。負荷分散は、送信元 IP アドレスに基づいて、1時間持続して行われます。同じ送信元 IP アドレスから送信された 2つの要求の間隔がこの持続時間を上回ると、バランシングは再決定されます。トラフィックの分散は単純なラウンドロビンアルゴリズムに基づいています。

サーバープールのすべてのサーバーは ICMP ping、TCP 接続の確立、または HTTP/S 要求により監視されます。障害が発生すると、影響を受けたサーバーは負荷分散に使用されなくなり、問題と考えられる送信元 IP の持続性は却下されます。

> **注 –** HTTP/S要求のリターンコードは`1xx Informational`、`2xx Success`、`3xx Redirection`、または`4xx Client Error`のいずれかであることが必要です。その他のすべてのリターンコードは障害の発生を意味します。

8.5.1 分散ルール

*ネットワークプロテクション > サーバロードバランシング > 分散ルール*タブで、Sophos UTMソフトウェアの負荷分散ルールを作成できます。ルールの作成後、サーバ間での重み分散を追加で定義し、インタフェースパーシスタンスを設定することができます。

負荷分散のルールを作成するには、以下の手順に従います。

1. ***負荷分散ルール*タブで、*新規負荷分散ルール*をクリックします。**
   *負荷分散ルールの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   サービス: 負荷分散するネットワークサービスです。

   仮想サーバ: 受信トラフィックの元のターゲットホスト。このアドレスは通常、ゲートウェイの外部アドレスと同じになります。

   リアルサーバ: 交替でサービスのトラフィックを受け付けるホスト。

   ヒント – 定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

   チェックタイプ: サービスをモニタリングするためのチェックタイプを、以下から1つ選択します。

   - **TCP:**TCP接続の確立
   - **UDP:**UDP接続の確立
   - **Ping:**ICMP Ping
   - **HTTP Host:**HTTP要求
   - **HTTPS**ホスト**:**HTTPS要求

   *UDP*を使用する場合、ping要求が最初に送信され、成功した場合は、続いてペイロード0のUDPパケットが送信されます。pingが成功しなかった場合や、ICMPポートに到達できない場合、このサーバはダウンしているとみなされます。*HTTP*および*HTTPS*要求の場合は、*URL*を入力できます。ホスト名は指定してもしなくても構いません(例:`index.html`あるいは`http://www.example.com/index.html`)。

   間隔: チェック間隔を秒単位で入力します。デフォルトは15秒です。つまり15秒ごとに、すべての本サーバの健全性状態がチェックされます。

   タイムアウト: 本サーバが応答を送信する最大時間を秒単位で入力します。本サーバがこの時間内に応答しない場合、デッドとみなされます。

   自動ファイアウォールルール(オプション): このチェックボックスは、ゲートウェイルールを自動生成する場合に選択します。これらのルールにより、トラフィックをホストから実際のサーバに送ることができます。

仮想サーバアドレスのシャットダウン(オプション):このチェックボックスは、追加のアドレスを負荷分散用の仮想サーバとして使用する場合(*インターフェース > 追加アドレス*の章を参照)にのみ使用できます。すべてのリアルサーバが利用不可になった場合、追加アドレスインタフェースは自動的にシャットダウンされます。

コメント(オプション):説明などの情報を追加します。

3. ***保存*をクリックします。**
新しいルールが*負荷分散*リストに表示されます。

負荷分散ルールを有効にします。

4. 新しいルールはデフォルトで無効になっています(トグルスイッチはグレー表示)。ルールを有効にするには、トグルスイッチをクリックします。
これでルールが有効になります(トグルスイッチは緑色)。

ルールを編集または削除するには、対応するボタンをクリックします。

例:それぞれ`192.168.66.10`および`192.168.66.20`というIPアドレスの2台のHTTPサーバがDMZにあるとします。ゲートウェイの外部インタフェースで受信したHTTPトラフィックを両方のサーバに均等に分散したいと仮定します。負荷分散ルールをセットアップするには、各サーバのホスト定義を選択あるいは作成します。それらを*http_server_1*および*http_server_2*とします。次に、*新規負荷分散ルールの作成*ダイアログボックスで、*サービス*として*HTTP*を選択します。さらに、*仮想サーバ*としてゲートウェイの外部アドレスを選択します。最後に、*リアルサーバ*ボックスにホスト定義を入力します。

荷重分散およびインタフェースパーシスタンス

負荷分散サーバ間で荷重を分散し、それらの間にインタフェースパーシスタンス設定するには、以下の手順に従ってください。

1. **負荷分散ルールの*編集*ボタンをクリックします。**
*負荷分散ルールの編集*ダイアログボックスが開きます。

2. ***リアルサーバ*ボックスのヘッダでスケジューラボタンをクリックします。**
*スケジューラの編集*ダイアログボックスが開きます。

3. **次の設定を行います。**
荷重:荷重とは、あるサーバが処理するトラフィック量を他のサーバに対して相対的に示すもので、0～100の間で設定できます。荷重ラウンドロビンアルゴリズムが使用され、値が大きいほど、該当サーバにルーティングされるトラフィックが多くなります。相対的な値であるため、合計して100にする必要はありません。たとえば、サーバ1の値を100に、サーバ2の値を50に、サーバ3の値を0に設定することなどができます。この場合、サーバ2のトラフィック量はサーバ1の半分となり、サーバ3は他のサーバが使用可能でない場合にのみ使用されま

す。0の値は、より値が大きい他のサーバが常に使用されることを示します(他のインタフェースが使用可能であれば)。

インタフェースパーシステンス: インタフェースパーシスタンスとは、クライアントからの後続の接続が常に同じアップリンクインタフェース経由でルーティングされるようにする技術です。パーシスタンスのデフォルトのタイムアウト時間は1時間です。この負荷分散ルールのインタフェースパーシスタンスを無効化することもできます。

4. ***保存*をクリックします。**
   *スケジューラの編集*ダイアログボックスが終了し、設定が保存されます。

5. ***保存*をクリックします。**
   *負荷分散ルールの編集*ダイアログボックスが閉じます。

8.6 VoIP

VoIP *Voice over Internet Protocol* は、インターネットまたは他のIPベースのネットワークを通した音声会話のルーティングです。Sophos UTMは、IPネットワーク上で音声信号を伝送するために最もよく使用される次のプロトコルのサポートを提供しています。

- SIP
- H.323

8.6.1 SIP

Session Initiation Protocol(SIP)は2つ以上の通信パートナー間のセッションの設定、変更、および終了のための信号を送るプロトコルです。SIPは主に音声または音声通話の確立と終了処理に使用します。SIPを使用するには、まずIP アドレスとURLをISPで登録する必要があります。SIPは、UDPまたはTCPをポート`5060`で使用して、どのIP アドレスおよびポート番号をエンドポイント間でのメディアデータ交換(ビデオや音声)で使用するべきかを示します。すべてのアドレスのすべてのポートを開くとセキュリティに重大な問題が生じるため、ゲートウェイでSIPトラフィックをインテリジェントに処理することができます。これは、特別なコネクショントラッキングヘルパによって実現します。このヘルパは制御チャネルをモニタリングし、どの動的ポートが現在使用されているかを判断して、制御チャネルがビジーであるときはこれらのポートのみをトラフィックが通過するようにします。これを行うために、SIPプロトコルを介した通信を可能にする適切なファイアウォールルールを作成するために、SIPサーバとSIP クライアントネットワーク定義の両方を指定する必要があります。

SIPプロトコルのサポートを有効にするには、以下の手順に従います。

1. ***SIP*タブで、SIPプロトコルのサポートを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、*グローバルSIP設定*エリアが編集可能になります。

2. **次の設定を行います。**
   SIPサーバネットワーク **SIP Server Networks** ：ここで、SIPクライアントの接続先として許可されるSIPサーバ（ISPが提供）を選択します。セキュリティ上の理由から、*すべて*は選択しないでください。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

   SIP クライアントネットワーク: SIP通信の開始や応答を許可されるSIPクライアントのホスト/ネットワークを追加または選択します。SIPクライアントとはLAN内のエンドポイントであり、他のSIPクライアントとのリアルタイムな双方向通信に関与します。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

   予想モード: 通信セッションの初期化を制限する方法を選択します。

   - 厳密 : 受信コールは、ISPのレジストラからの場合だけ許可されます。例、例、REGISTER SIP メッセージが送信されたIP アドレス加えて、UTMは、信号エンドポイントからのメディア（音声またはビデオ）データしか受け入れません。つまり、SIP メッセージを実行したデバイスのことです。UTM一部のプロバイダは、SIP メッセージ以外のIP からのメディアデータを送信しますがによって拒否されます。
   - クライアント/サーバネットワーク: 定義済みSIP サーバまたはクライアントのネットワークのすべてのクライアントからの受信コールが許可されます。定義済みSIP サーバまたはクライアントのネットワークのアドレスであれば、SIP メッセージを送信した送信者以外の送信者のIP アドレスからのメディアデータが許可されます。
   - すべて: どこからの受信コールならびにメディアデータであっても許可されます。

3. ***適用*をクリックします。**
   設定が保存されます。

   トグルスイッチが緑色に変わります。

設定をキャンセルするには、アンバー色のトグルスイッチをクリックします。

8.6.2 H.323

H.323とは、ITU-T *国際電気通信連合* が公開した国際マルチメディア通信プロトコル標準であり、あらゆるパケット交換網上で音声・映像通信セッションを提供するプロトコルを規定しています。H.323は、VoIP *ボイスオーバーIP* やIPベースのテレビ会議で一般的に使用されます。

H.323では、ポート`1720`でTCPを使用して、エンドポイント間で使用する動的ポート範囲をコールのセットアップ時にネゴシエートします。動的範囲内ですべてのポートを開くと、セキュリティ上で重大な問題が発生するため、ゲートウェイはインテリジェントベースでH.323関連のトラフィックを許可することができます。これは、特別なコネクショントラッキングヘルパによって実現します。このヘルパは制御チャネルをモニタリングし、どの動的ポートが現在使用されているかを判断して、制御チャネルがビジーであるときはこれらのポートのみをトラフィックが通過するようにします。この目的を達成するためには、H.323プロトコルでの通信を可能にする適切なファイアウォールルールを作成するために、H.323ゲートキーパとクライアントネットワーク定義の両方を指定する必要があります。

H.323プロトコルのサポートを有効にするには、以下の手順に従います。

1. ***H.323*タブで、H.323プロトコルのサポートを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、*グローバルH.323設定*エリアが編集可能になります。

2. **次の設定を行います。**
   H.323ゲートキーパ: H.323ゲートキーパを追加または選択します。H.323ゲートキーパは、ゾーン内のすべてのH.323クライアント（マイクロソフトのNetMeetingなどのエンドポイント）をコントロールします。より具体的には、ゲートキーパはLAN上のゾーン内のすべてのH.323コールに対するモニタとして機能します。ゲートキーパの最重要タスクは、シンボルエイリアスアドレスとIPアドレスとの変換です。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

   H.323クライアント: ここで、H.323接続を開始する元のホスト/ネットワークと宛先のホスト/ネットワークを追加または選択できます。H.323クライアントとはLAN内のエンドポイントであり、他のH.323クライアントとのリアルタイムな双方向通信に関与します。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

3. ***適用*をクリックします。**
   設定が保存されます。

   トグルスイッチが緑色に変わります。

設定をキャンセルするには、アンバー色のトグルスイッチをクリックします。

8.7 詳細

ネットワークプロテクション > *詳細*メニューのタブを使用すると、ジェネリックプロキシ、SOCKSプロキシ、IDENTリバースプロキシなど追加のネットワークプロテクション機能を設定することができます。

8.7.1 ジェネリックプロキシ

ジェネリックプロキシ（別名「ポートフォワーダ」）は、DNATとマスカレーディングの両機能を組み合わせており、特定のサービスへのすべての受信トラフィックを任意のサーバに転送（フォワーディング）します。標準DNATとの違いは、ジェネリックプロキシでは送信接続についても要求の送信元IPアドレスをインタフェースのIPアドレスに書き換える点です。さらに、宛先（ターゲット）ポート番号も変更することができます。

ジェネリックプロキシルールを追加するには、次の手順に従います。

1. ***ジェネリックプロキシ*タブで、*新規ジェネリックプロキシルール*をクリックします。**
   *ジェネリックプロキシルールの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   インタフェース: 受信接続のインタフェースを選択します。

   サービス: プロキシを使用するトラフィックのサービス定義を追加または選択します。

   ホスト: トラフィックの転送先とするターゲットホストを追加または選択します。

   サービス: プロキシを使用するトラフィックのターゲットサービスを追加または選択します。

   許可ネットワーク: ポート転送を適用するネットワークを追加または選択します。

   ヒント – 定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

   コメント（オプション）: 説明などの情報を追加します。

3. ***保存*をクリックします。**
   *ジェネリックプロキシ*ルールリストに表示されます。

   ジェネリックプロキシルールを有効にします。
4. 新しいルールはデフォルトで無効になっています（トグルスイッチはグレー表示）。ルールを有効にするには、トグルスイッチをクリックします。これでルールが有効になります（トグルスイッチは緑色）。

ルールを編集または削除するには、対応するボタンをクリックします。

8.7.2 SOCKSプロキシ

SOCKSとは、クライアントサーバ型アプリケーションがネットワークファイアウォールのサービスを透過的に使用できるようにするインターネットプロトコルです。ファイアウォール内にある多くのクライアントアプリケーションが、インターネット上のホストと通信するために使用します。例としては、IRC/インスタントメッセージングクライアント、FTPクライアントや、Windows SSH/Telnetクライアントです。ファイアウォールの内側にあるこれらのクライアントは、外側にあるサーバにアクセスしたい場合、その代わりにSOCKSプロキシサーバに接続します。このプロキシサーバは、クライアントが外部サーバにアクセスする適格性をコントロールし、要求をサーバに受け渡します。クライアントアプリケーションは、SOCKS 4またはSOCKS 5というプロトコルバージョンを明示的にサポートしている必要があります。

SOCKSのデフォルトポートは`1080`です。ほぼすべてのクライアントにこのデフォルトポート設定が導入されているため、通常は設定不要です。SOCKSとNATの違いは、SOCKSが「バインド」要求(クライアントの代わりにポートでリスンする機能。わずかなクライアントだけがこれをサポートしています)もサポートしており、SOCKS 5ではユーザ認証が可能である点です。

SOCKSプロキシを有効にする場合、プロキシへのアクセス権がある1つ以上のネットワークを定義しなければなりません。ユーザ認証が必要である場合、SOCKSプロキシの使用を許可するユーザまたはグループも選択する必要があります。

注 **-** ユーザ認証を使用しない場合、SOCKSプロキシはSOCKS 4プロトコルとSOCKS 5プロトコルの両方で使用できます。ユーザ認証を選択した場合、SOCKS 5のみが機能します。プロキシにSOCKS 5モードでホスト名を解決させる場合、DNSプロキシも有効にする必要があります。有効にしないと、DNS解決は失敗します。

SOCKSプロキシを設定するには、次の手順に従ってください。

1. ***SOCKSプロキシ*タブで、SOCKSプロキシを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、*SOCKSプロキシオプション*エリアが編集可能になります。

2. **次の設定を行います。**
   許可ネットワーク: SOCKSプロキシの使用を許可するネットワークを追加または選択します。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

ユーザ認証の有効化:このオプションを選択すると、ユーザはSOCKSプロキシへのログイン時にユーザ名とパスワードを入力しなければならなくなります。ユーザ認証をサポートしているのがSOCKS 5のみであるため、SOCKS 4は自動的に無効になります。

許可されたユーザ:SOCKSプロキシの使用を許可するユーザまたはグループを選択するか、新しいユーザを追加します。ユーザを追加する方法は、*定義とユーザ* > *ユーザとグループ* > *ユーザ*ページで説明しています。

3. ***適用*をクリックします。**
   設定が保存されます。

   トグルスイッチが緑色に変わります。

8.7.3 IDENT リバースプロキシ

IDENTプロトコルは、リモートサーバがアクセス元クライアントの身元を簡単に確認するために使用します。IDENTプロトコルは暗号化されず、スプーフィングが簡単ですが、多くのサービスではいまだにこのプロトコルを使用しており、場合によっては必須です。

IDENTリレーを設定するには、次の手順に従ってください。

1. ***IDENT リバースプロキシ*タブで、IDENTリレーを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチが緑色になり、*グローバル設定*エリアが編集可能になります。

2. **次の設定を行います。**
   内部ホストへの転送(オプション):IDENTクエリはゲートウェイの接続追跡でカバーされないため、マスカレーディングが使用されている場合は「スタック」します。ゲートウェイの内側にあるマスカレーディングされたホストにIDENTクエリを受け渡すためには、*内部ホストへの転送*オプションを選択します。実際のIP接続は転送されません。代わりに、ゲートウェイが内部クライアントにIDENT応答を要求し、その文字列を要求元サーバに転送します。この方法は、主要IRCクライアントとFTPクライアントに組み込まれた大部分の「ミニIDENT」サーバで機能します。

   デフォルト応答:IDENTリレーを有効にすると、ゲートウェイはIDENT要求への応答をサポートします。システムは、接続を開始したローカルサービスを問わず常に、*デフォルト応答*ボックスに入力した文字列で応答します。

3. ***適用*をクリックします。**
   設定が保存されます。

9 Webプロテクション

この章では、Sophos UTMの基本Webプロテクション機能の設定の仕方を説明します。

この章には次のトピックが含まれます。

- Webフィルタリング
- Webフィルタプロファイル
- フィルタリングオプション
- ポリシテスト
- アプリケーションコントロール
- FTP

Webadminの*Webプロテクション統計*ページには、時間、トラフィック、ならびに上位ユーザのアクセス状況に基づいて、最も使用されたアプリケーションやアプリケーションカテゴリ、最もアクセスの多いドメインの概要が表示されます。さらに、ブロックされた上位Webサイトカテゴリが表示されます。各セクションには*詳細*リンクがあります。リンクをクリックするとWebAdminのそれぞれのレポーティングセクションが表示され、そこでさらなる統計情報を参照できます。

注 – Web使用状況データがどのようにして収集され、*ログとレポート > Webプロテクション > Web使用状況レポート*ページで統計がどのように算出されているかについての詳細情報を見つけられます。

*上位アプリケーション*セクションでは、アプリケーション名の上にカーソルを合わせると、追加機能が1つまたは2つ表示されます。

- *ブロック*アイコンをクリックすると、現時点から該当アプリケーションがブロックされます。これにより、*アプリケーション制御ルール*ページにルールが作成されます。このオプションは、Sophos UTMの正常なオペレーションに必要なアプリケーションに対しては利用できません。たとえば、WebAdminトラフィックはブロックできません。これをブロックすると、ユーザ自身がWebAdminからシャットアウトされてしまいます。未分類のトラフィックもブロックできません。
- *シェーピング*アイコンをクリックすると、それぞれのアプリケーションのトライフィックシェーピングが有効になります。ダイアログウィンドウが開き、ルール設定を定義するよう要求されます。完了したら*保存*をクリックします。これにより、*および帯域幅プール*ページの両方にルールが作成されます。シェーピングはインタフェース単位で機能するため、*すべてのインタフェース*フローモニタを閲覧している際はトラフィックシェーピングを利用できません。

- *帯域幅調整*アイコンをクリックして、対応するアプリケーションのトラフィック帯域幅調整を有効化します。ダイアログウィンドウが開き、ルール設定を定義するよう要求されます。完了したら*保存*をクリックします。これにより、*トラフィックセレクタ*および*ダウンロード帯域幅調整*ページにルールが作成されます。ダウンロード帯域幅調整はインタフェース単位で機能するため、*すべてのインタフェース*フローモニタを閲覧している際はダウンロード帯域幅調整を利用できません。

9.1 Webフィルタリング

*Webプロテクション > Webフィルタリング*メニューのタブを使用すると、Sophos UTMをHTTP/Sキャッシングプロキシとして設定することができます。これには、送受信Webトラフィックをスキャンし、スパイウェアから保護し、悪意のあるWebサイトを検出する、ウイルス対策が含まれています。また、異なるカテゴリのWebサイトへのアクセスを制御できますので、管理者は、ギャンブル、ポルノ、ショッピングといったものへのアクセスに関するポリシを強制し、これらのサイトのブロックまたはクリックスルー警告ページの提供が可能です。

Sophosのエンドポイントソフトウェアと合わせて使用することで、Sophos UTMは外部ネットワークにあるエンドポイントマシンでも同じWebポリシを適用し、監視することができます。ユーザはラップトップを家に持ち帰る、または出張に携帯することが可能であり、同じポリシが適用されます。*エンドポイントWebコントロール*を有効にするには、*エンドポイントプロテクション > Webコントロール*を参照してください。

引き続き、フィルタのアクションを*Webフィルタプロファイル > フィルタアクション*タブで管理することができます。そこで、フィルタアクションを追加、変更、複製、削除することができます。ただし、*Webフィルタリング > ポリシ*タブで*フィルタアクションの追加/編集*ウィザードを起動することで、フィルタアクションを作成、変更、割り当ることができます。

9.1.1 Webフィルタリングの変更

9.2リリースの時点で、Sophos UTMには、Webフィルタリングポリシの作成および管理のための新しい簡素化されたインタフェースが含まれています。インタフェースはかなり変更されていますが、機能は変わっていません。既存の設定はすべて保存され、システムに変更がなければ、まったく同様に動作します。

以前は、複雑なWebポリシにWebフィルタリングプロファイルの作成が関与していました。これらが、*フィルタアクション*タブで作成されるフィルタアクションを構成し、*フィルタ割当て*タブでのフィルタ割当てを通じてユーザやグループに割り当てられ、*プロキシプロファイル*タブで設定されていました。

現在は、デフォルトの構成や詳細なフィルタリングプロファイルを含めて、*Web フィルタリング > ポリシ*タブでWebフィルタリングポリシのあらゆる側面を設定できます。

注 – 少し時間を取って、新しいインタフェースに習熟してから、以下の概要を読んでください。以前のリリースとは異なりますが、複雑なWebポリシが簡単に作成、管理できるはずです。

9.1.1.1 重要な変更点

- In 9.1では、*Webプロテクション > Web フィルタリング*に位置していた、グローバルオプションを含む複数のタブがありました。これらのタブは、*Webプロテクション > フィルタリングオプション*へと移動されました。
- 9.1では、プロキシプロファイルにはフィルタ割当てがあり、条件に基づき異なるフィルタアクションを選択できました。これらはポリシを有するフィルタプロファイルと呼ばれるようになり、プロファイルの2番目のタブ上の表に示されます。
- 9.1では、デフォルトプロファイルは単一フィルタ割当て(デフォルト割当て)しかサポートしていませんでした。これからは、デフォルトプロファイルで複数のポリシを持つことができます。
- 9.1では、各プロファイルにフォールバックアクションがありました。これは基本ポリシと呼ばれるようになりましたが、機能は同じです。基本ポリシには、他のポリシが一致しない場合に使用されるフィルタアクションが含まれています。
- 9.1では、デフォルトプロファイル上の複数のタブを使用してフィルタアクションを作成していましたが、追加を行うとスクロール域が非常に縦長になっていました。今後すべてのフィルタアクションの作成は、複数のタブによる対話型処理、*フィルタアクションウィザード*で行われます。

9.1.1.2 一般的なタスク

以下は、9.1インタフェースとの対比を含めて、9.2およびそれ以降で一般的なタスクを実行する方法の簡単な概要です。

実行方法:	9.1	9.2
デフォルトポリシを編集しますか?	*Webフィルタリング*のさまざまなタブを設定する: • *Webフィルタリング > ウイルス対策/マルウェア* • *Webフィルタリング > URLフィルタリング* • *Webフィルタリング > 詳細*	*Webフィルタリング > ポリシ*
プロキシプロファイルを作成または編集しますか?	*Webフィルタリングプロファイル > プロキシプロファイル*	*Webフィルタリング > Webフィルタリングプロファイル*
プロキシプロファイルにフィルタ割当てを割当てますか?	1. *Webフィルタリングプロファイル > フィルタアクション*で、フィルタアクションを作成 2. *Webフィルタリングプロファイル > フィルタ割り当て*で、フィルタ割り当てを作成 3. *Webフィルタリングプロファイル > プロキシプロファイル*でプロキシプロファイルを編集または追加	1. *Webフィルタリングプロファイル > フィルタプロファイル*で、*フィルタプロファイル*の名前をクリックするか、緑の「+」アイコンをクリックしてプロファイルを作成 2. *ポリシ*タブで、緑の「+」アイコンをクリックしてポリシを追加。 3. *フィルタアクション*を選択するか、緑の「+」アイコンをクリックして1つ作成する。
Webサイトをデフォルトフィルタアクション内のブラックリストに追加しますか?	*Webフィルタリングプロファイル > フィルタ割り当て*	*Webフィルタリング > ポリシ*で、ポリシの作成または編集の際に、*フィルタアクション*の横にある緑の「+」アイコンをクリックします。

実行方法：	9.1	9.2
自分のフィルタ割り当てに新しいフィルタアクションを作成しますか？	*Web フィルタリング > URL フィルタリング*で、*ブロックする追加 URL/サイト*の横にある緑の「+」アイコンをクリックします。	1. *Web フィルタリング > ポリシ* 2. *デフォルトコンテンツフィルタアクション*を選択します 3. *Web サイト*タブで、*これらのWeb サイトをブロック*の横にある緑の「+」アイコンをクリックします。
詳細設定を変更しますか？	*Web フィルタリング > 詳細*	*フィルタオプション > その他*
信頼されるHTTPS CAを管理しますか？	*Web フィルタリング > HTTPS CA*	*フィルタリングオプション > HTTPS CA*

9.1.1.3 移行

バージョン9.2にアップグレードすると、以前の構成および設定は保存され、システムは引き続き同様に動作します。ただし、インタフェースが大幅に変更されているので、必ずしもすべてが予想通りではないかもしれません。*Web フィルタリング*メニューアイテムには、許可ネットワークに対してポリシおよびアクションを適用すべき、すべての設定が含まれています。*Web フィルタプロファイル*メニューアイテムには、対応する設定が含まれていますが、複数のプロファイルを作成できますので異なる設定を異なるネットワークに適用可能です。すべてのグローバル設定は今後、*フィルタリングオプション*メニューアイテムのタブ上に表示されます。

一部のオブジェクトの名前が変わりました。例えば、*プロキシプロファイル*は*フィルタプロファイル*、*フィルタ割当て*は*ポリシ*と呼ばれるようになりました。*フォールバックアクション*は今後*基本ポリシ*と呼ばれます。なぜなら、その他のポリシが一致しない場合に起こるポリシ/アクションだからです。すべての*ポリシ*がプロファイルの1つのタブ上に表示されるようになりましたので、これらのオブジェクト間の関係がより明確になっています。*フィルタアクション*は、アクションについて設定可能なすべてのアイテムを含む、ポップアップタブ式のダイアログを使用して追加または変更できます。

9.1の限界の1つとして、デフォルトプロファイルにユーザグループを1つしか設定できなかったことが挙げられます。これは、*デフォルトコンテンツフィルタプロファイル割当て*と呼ばれるポリシに移行され、*デフォルトコンテンツフィルタアクション*と呼ばれる移行フィルタアクションが付いています。その他のフィルタ割当てを作成した場合、これらはプロファイル内に無効なポリシとして表示されるようになります。

9.1では、複数の割当てを持つためだけにプロファイルを作成する場合、これらのポリシを最初のメニューオプションのデフォルトプロファイルで有効化して、設定を簡素化できます。*許可ネットワーク*が正しいことを確認し、その後、不必要となった追加プロファイルを削除します。

9.1.2 グローバル

Webプロテクション > *Webフィルタリング* > *グローバル*タブでは、Webフィルタのグローバル設定を実行できます。

Web フィルタを設定するには、次の手順に従います。

1. ***グローバル*タブで、Webフィルタを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチが緑色になり、*プライマリWebフィルタプロファイル*エリアが編集可能になります。

2. **許可するネットワークを選択します。**
   Webフィルタの使用を許可するネットワークを選択します。デフォルトで、WebフィルタはクライアントアントProxy要求をTCPポート8080でリスンし、*許可ネットワーク*ボックスにリストされたネットワーク内のすべてのクライアントに対して接続を許可します。

   警告 – セキュリティリスクを招き、インターネットの悪用に道を開くので、決してネットワークオブジェクトで*すべて*を選択しないでください。

3. **HTTPS(SSL)トラフィックのオプションを選択する。**
   SSLトラフィックのスキャンは次のオプションから選択:

   - *スキャンしない*:このオプションは、透過モードのみで使用可能です。選択した場合、HTTPSトラフィックはプロキシを経由せず、スキャンは実施されません。
   - *URLフィルタリングのみ*:このオプションは、URLカテゴリおよび評判チェックが実行されますが、HTTPSトラフィックのコンテンツのスキャンは実施されません。
   - *複合化およびスキャン*:このオプションを選択した場合、HTTPSトラフィックの複合化および完全チェックが実行されます。

4. **オペレーションのモードを選択します。**
   ユーザ認証が必要なオペレーションモードを選択する場合には、Webフィルタの使用を許可するユーザとグループを選択する必要があります。次のオペレーションモードを使用できます。

- 標準 : 標準モードでは、Webフィルタはデフォルトでクライアント要求をポート8080でリスンし、*送信元ネットワーク*ボックスにリストされたネットワーク内のすべてのクライアントに対して接続を許可します。このモードで使用する場合、クライアントはブラウザの設定でWebフィルタにHTTPプロキシを指定していることが必要です。

  デフォルトの認証モードを選択します。

  - なし: 認証をしない場合に選択します。
  - **Active Directory SSO**: このモードでは、コンピュータにプロキシのユーザとして現在ログインしている(シングルサインオン)ユーザの認証が試行されます。現在ログインしているユーザがプロキシ使用許可を持つ有効なADユーザである場合、認証はユーザインタラクションなしで行われるはずです。*定義とユーザ > 認証サービス > サーバ*タブで、*Active Directory シングルサインオン Active Directory Single Sign-On* (SSO)が設定されていなければなりません。クライアントはNTLMまたはKerberosで認証可能です。
  - エージェント: SophosAuthentication Agent(SAA)を使用する場合に選択します。Webフィルタを使用するためには、エージェントと認証を開始する必要があります。エージェントは、ユーザポータルからダウンロードできます。ユーザポータルをご覧ください。
  - **Apple OpenDirectory SSO**: *定義とユーザ > 認証サービス > サーバタブでLDAP*を設定しており、Apple OpenDirectoryを使用している場合、これを選択します。さらに、プロキシが正しく機能するようにするためには、*Webプロテクション > フィルタリングオプション > その他*タブで、MAC OS Xシングルサインオン Kerberos鍵ファイルをアップロードする必要があります。このモードで使用する場合、クライアントはブラウザの設定でWebフィルタにHTTPプロキシを指定していることが必要です。Safariブラウザは SSOをサポートしていません。
  - 基本ユーザ認証 : このモードでは、各クライアントはプロキシを使用する前にこのプロキシに対して自己認証する必要があります。サポートされる認証方式について詳しくは、*定義とユーザ > 認証サービス*を参照してください。このモードで使用する場合、クライアントはブラウザの設定でWebフィルタにHTTPプロキシを指定していることが必要です。
  - ブラウザ : 選択すると、Webフィルタへの自己認証のためのログインダイアログがユーザのブラウザに表示されます。このモードでは、クライアント側のブラウザ設定なしで、ユーザ名に基づく追跡、報告、およびサーフィンが可能になります。さらに、そのダイアログウィンドウに追加で免責条項を表示することができます。この場合、ユーザが先に進むためには、免責条項に同意する必要が

あります。免責条項について詳しくは、*マネジメント> カスタマイズ > Web メッセージ*の章を参照してください。

- **eDirectory SSO**: *定義とユーザ > 認証サービス > サーバ*タブで*eDirectory*を設定した場合、これを選択します。

注 – eDirectoryのシングルサインオン(SSO)モードの場合、Webフィルタはアクセス先のIPアドレスと資格情報を最大15分間キャッシュします。Apple OpenDirectory SSOの場合、キャッシュできるのはグループ情報のみです。これは、認証サーバへの負荷を軽減するために行われます。逆に言うと、ユーザ、グループ、またはアクセスしているユーザのログインステータスの変更がWebフィルタによって反映されるまで、最大15分かかります。

ユーザ認証が必要な認証モードを選択した場合は、*認証失敗のアクセスをブロック*を選択し、認証を失敗したユーザのアクセスを拒否します。

- 透過モード: 透過モードでは、ポート80(SSLを使用している場合はポート443)でクライアントブラウザアプリケーションが行うすべての接続はインターセプトされ、クライアント側の設定なしでWebフィルタにリダイレクトされます。クライアントがWebフィルタサーバを意識することは全くありません。このモードのメリットは、多くのインストールについては、その他の管理やクライアント側の設定が必要ないということです。しかし、処理可能なのはHTTP要求のみという短所があります。そのため、透過モードを選択すると、クライアントのプロキシ設定は無効になります。

注 – 透過モードでは、WebフィルタはHTTP要求からNTLM認証ヘッダを削除します。さらに、WebフィルタはこのモードではFTP要求を処理できません。クライアントがこのようなサービスにアクセスする必要がある場合は、ファイアウォールでポート(21)を開く必要があります。一部のWebサーバは、ポート80以外のポート経由でストリーミング動画や音声などのデータを送信します。これらの要求は、Webフィルタが透過モードで機能しているときは検知されません。このようなトラフィックにも対応したい場合には、他のモードを使用するか、これらを許可する明確なファイアウォールルールを入力する必要があります。

  - なし: 認証をしない場合に選択します。
  - **Active Directory SSO**: このモードでは、コンピュータにプロキシのユーザとして現在ログインしている(シングルサインオン)ユーザの認証が試行されます。現在ログインしているユーザがプロキシ使用許可を持つ有効なADユーザ

である場合、認証はユーザインタラクションなしで行われるはずです。*定義とユーザ* > *認証サービス* > *サーバ*タブで*Active Directoryシングルサインオン SSO* を設定する必要があります。クライアントは、NTLM(またはMacの場合はKerberos)を使用して認証を行えます。一部の環境については、エンドポイントの追加設定が必要です。透過モードでSSOに関する問題がある場合、Sophos Knowledgebase Article 120791をご覧ください。

> 注 – Active Directoryユーザグループを定義する場合、LDAP文字列の代わりにプレーンなActive Directoryのグループまたはユーザの名前を手動で入力することで、*Active Directoryグループ*ボックスに必要なエントリを追加することを強く推奨いたします。例:LDAP文字列`CN=ads_group1,CN=Users,DC=example,DC=com`の代わりに、単に名前`ads_group1`を入力します。

> 注 – Kerberosを使用している場合は、ユーザを入力することをWebフィルタが許可していないので、単にグループを*Active Directoryグループ*ボックスに追加するだけです。

- エージェント: SophosAuthentication Agent(SAA)を使用する場合に選択します。Webフィルタを使用するためには、エージェントと認証を開始する必要があります。
- ブラウザ: 選択すると、Webフィルタへの自己認証のためのログインダイアログがユーザのブラウザに表示されます。このモードでは、クライアント側のブラウザ設定なしで、ユーザ名に基づく追跡、報告、およびサーフィンが可能になります。さらに、そのダイアログウィンドウに追加で免責条項を表示することができます。この場合、ユーザが先に進むためには、免責条項に同意する必要があります。免責条項について詳しくは、*マネジメント* > *カスタマイズ* > *Webメッセージ*の章を参照してください。

- フル透過 (オプション): クライアントの送信元IPをゲートウェイのIPに置き換えず、そのまま維持する場合は、選択します。これは、クライアントがパブリックIPアドレスを使用しており、Webフィルタによって隠すべきではない場合に便利です。このオプションはブリッジモードでの実行中においてのみ利用可能です。

  *フル透過*で利用可能な認証モードは、*透過*と同じです。上記をご覧ください。

認証の使用を設定する場合、*認証失敗のアクセスをブロック*するオプションがあります。AD SSOを使用中で認証失敗のアクセスをブロックしない場合、SSOの認証失敗により、ユーザ

プロンプトなしで未認証のアクセスが許可されてしまいます。ブラウザ認証を使用中で認証失敗のアクセスをブロックしない場合、ログインページに追加の*ゲストログイン*リンクが現れ、未認証のアクセスが許可されます。

5. **デバイス固有の認証を有効にする。**
   特定のデバイスの認証モードを設定するには、*デバイス固有の認証を有効にする*チェックボックスを選択します。有効になると、緑の「+」アイコンをクリックして、デバイスのタイプや関連する認証モードを追加することができます。

6. ***適用*をクリックします。**
   設定が保存されます。

重要 – SSLスキャニングを透過モードと組み合わせて有効にすると、一部のSSL接続(SSL VPNトンネルなど)が失敗します。SSL VPN接続を有効にするには、対応するターゲットホストを*透過モードスキップリスト*に追加します(*Webプロテクション > フィルタリングオプション > その他*を参照)。さらに、自己署名証明書でホストにアクセスするには、*証明書信頼性チェック*オプションを選択して、これらのホストの除外を作成する必要があります。これにより、プロキシで証明書のチェックが行われません。

ライブログ

Webフィルタリングライブログは、Web要求に関する情報を提供します。*ライブログを開く*ボタンをクリックすると、新しいウィンドウでWebフィルタリングライブログが開きます。

9.1.3 HTTPS

*Webプロテクション > Webフィルタリング > HTTPS*タブで、WebフィルタリングによるHTTPSトラフィックの処理方法を設定できます。

- **URL***フィルタリングのみ*: このオプションを選択すると、カテゴリのドメイン名、タグ、サイトがホワイトリスト/ブラックリストに載っているかどうかに基づき、フィルタリングされます。
- *復号化してスキャン*: URLフィルタリングを実行し、フルスキャンのHTTPS復号化も実行するには、このオプションを選択します。
- *以下を復号化してスキャン*: URLフィルタリングを実行して、選択したカテゴリまたはタグ付きサイトを復号化しスキャンするには、このオプションを選択します。
  - *これらのタグ付けされた***Web***サイトをスキャンする*: このボックスを使用して、どのタグ付きサイトを復号化しスキャンするかを選択します。既存のタグを選択するには、フォルダアイコンを選択します。または「+」アイコンをクリックして、新規タグを追加します。既存のタグを追加するには、タグをを選択して*これらのタグ付けされたWebサイト*

*をスキャンする*リストボックスへとドラッグします。

- **これらの分類されたWebサイトをスキャンする**:このリストボックスを利用して、どのWebサイトカテゴリを復号化しスキャンするかを選択します。カテゴリをリストから削除するには、カテゴリの横のゴミ箱アイコンをクリックします。利用可能なカテゴリをリストするには、フォルダアイコンを選択します。カテゴリを追加するには、カテゴリを選択して*これらの分類されたWebサイトをスキャンする*リストボックスへとドラッグします。

- **透過モードでHTTPSトラフィックをプロキシしない**:すべてのHTTPSトラフィックのWebフィルタリングを無効化するには、このオプションを選択します。このオプションは、透過モードでのみ使用します。選択すると、WebフィルタはHTTPSトラフィックをプロキシしません。UTMを通じてHTTPSトラフィックを許可するにはファイアウォールルールを作成する必要があります。

9.1.4 ポリシ

Webプロテクション > *Webフィルタリング* > *ポリシ*タブを使用して、Webフィルタリングポリシの割り当てを作成、管理します。ポリシは特定のユーザ、グループまたは期間に異なるフィルタリングアクションを適用するために使用されます。これらのポリシは*グローバル*タブにある*許可ネットワーク*に適用されます。ユーザと時間に一致する最初のポリシが適用され、他に一致するものがない場合基本ポリシが適用されます。すべてのプロファイルに、最後に適用される基本ポリシがあり、無効にはできません。

新しいポリシを作成するには、以下の手順に従います。

1. **右上のプラス(+)アイコンをクリックします。**
   *ポリシの追加*ダイアログボックスが表示されます。

2. **次の設定を行います。**
   名前:このポリシを説明する名前を入力します。

   ユーザ/グループ:このポリシを適用させるユーザまたはユーザグループを選択します。また、新しいユーザまたはグループの作成もできます。ユーザを追加する方法は、*定義とユーザ* > *ユーザとグループ* > *ユーザ*ページで説明しています。

   時刻イベント:ポリシは、選択した期間の間有効になります。ポリシを常に有効にしておくには、*Always*を選択します。また、緑色の「+」アイコンをクリックして、新しい時刻イベントを作成することもできます。期間定義は、*定義とユーザ* > *期間定義*タブで管理します。

   フィルタアクション:既存のフィルタアクションを選択します。これにより、ポリシに適用させるWebプロテクションのタイプが定義されます。また緑色の「+」アイコンをクリックし、*フィルタアクションウィザード*を使用して新規フィルタアクションを作成することもできます。フィルタアクションも、*Webフィルタプロファイル* > *フィルタアクション*タブで管理できます。

コメント(オプション):説明などの情報を追加します。

詳細設定:

- 例外のため認証を省略したリクエストにポリシを適用する: *フィルタリングオプション* > *除外*タブで、例えば、認証を使用できない自動アップロードでの認証を省略するための例外を作成できます。このポリシを認証を省略したWebリクエストに適用する場合は、このチェックボックスを選択します。

3. ***保存*をクリックします。**
新しいポリシが *ポリシ*リストに表示されます。

4. **ポリシを有効にします。**
新規ポリシは、デフォルトで無効になっています(トグルスイッチは灰色)。ポリシを有効にするには、トグルスイッチをクリックします。これでポリシが有効になります(トグルスイッチは緑)。

- ポリシを変更するには、その名前をクリックします。
- ポリシが実行される順番を変更するには、右側にある上下矢印をクリックして、リストでポリシの位置を上下させます。
- フィルタのアクションを変更するには、フィルタのアクション名をクリックして、*フィルタアクションの編集*ウィザードを表示させるか、*Web フィルタプロファイル* > *フィルタアクション*タブに切り替えます。

9.1.4.1 フィルタアクションウィザード

*追加/編集 フィルタアクション*ウィザードは、Webポリシで使用するフィルタアクションの作成や編集のために使用します。このウィザードは、*ポリシの追加*または*ポリシの編集*ダイアログから起動するか、*Web フィルタリング* > *ポリシ*タブで既存のフィルタアクションの名前をクリックして起動します。

引き続き、フィルタのアクションを*Web フィルタプロファイル* > *フィルタアクション*タブで管理することができます。そこで、フィルタアクションを追加、変更、複製、削除することができます。ただし、*Web フィルタリング* > *ポリシ*タブで*フィルタアクションの追加/編集*ウィザードを起動することで、フィルタアクションを作成、変更、割り当ることができます。

9.1.4.2 カテゴリ

特定の種類のWebサイトへのアクセスをコントロールするデフォルトの設定を行います。

名前:このフィルタアクションを説明する名前を入力してください。

許可/ブロック:選択したWebサイトカテゴリを許可するかブロックするかを決定します。次のオプションを使用できます。

- 以下で指定したコンテンツ以外はすべて許可。
- 以下で指定したコンテンツ以外はすべてブロック。

*以下で指定したコンテンツ以外はすべて許可*を選択すると、すべてのカテゴリグループが*許可*にデフォルト設定され、*警告*、*ブロック*または*割当て*のいずれかに変更可能です。カテゴリグループの一部としてここに表示されていないカテゴリがある場合、それらも許可されます。Webサイトが複数カテゴリのメンバであり、いずれかのカテゴリがブロックされている場合、そのWebサイトはブロックされます。

*以下で指定したコンテンツ以外はすべてブロック*を選択すると、すべてのカテゴリグループが*ブロック*にデフォルト設定され、*警告*または*許可*のいずれかに変更可能です。カテゴリグループの一部としてここに表示されていないカテゴリがある場合、それらもブロックされます。Webサイトが複数カテゴリのメンバであり、いずれかのカテゴリが許可されている場合、そのWebサイトは許可されます。

注 – *割当て*に設定されているすべてのサイトカテゴリが、利用可能な割当て時間に対してカウントされます。利用可能な割当て時間は午前0時にリセットされます。または、*Webプロテクション > ポリシヘルプデスク > 割当てステータス*ページで手動でリセットできます。利用可能な割当て時間は、*フィルタアクションウィザード*の*追加オプション*ページで設定できます。

スパイウェアの伝染及び通信をブロック:このオプションを選択すると、スパイウェアカテゴリをブロックします。*すべてのコンテンツをブロック*している場合、これは常に選択されています。

注 – 高度な脅威検出により、追加のマルウェア通信を検出およびブロック可能です。これは、*ネットワークプロテクション > 高度な脅威防御 > グローバル*で設定できます。

カテゴリ:カテゴリごとに、Webサイトを訪問するユーザを許可するか、ブロックするか、ユーザが利用可能な割当て時間に対してカウントするかを設定できます。*警告*または*割当て*を選択した場合、該当カテゴリのサイトをブラウズするユーザにはまず警告ページが表示されますが、ユーザの選択でサイトへ進むことができます。

注 – デフォルトで18の「フィルタカテゴリ」へとグループ化されている、107のカテゴリがあります。これらは、*Webプロテクション > フィルタリングオプション > URLフィルタリングカテゴリ*で設定可能です。*フィルタアクションウィザード*に、設定済みのすべてのフィルタカテゴリが表示されます。

未分類のWebサイト:未分類のWebサイトは*許可*、*警告*、または*ブロック*されるべきです。

評判に基づきWebサイトをブロック: Webサイトは*信頼済み*、*ニュートラル*、*未確認*、*疑わしい*、または「悪意のある」に分類できますが、「悪意のある」はリストされていません。未分類のWebサイトを*未確認*と呼びます。使用しているネットワークからのアクセスを許可するために、Webサイトがどの評判を必要とするか選択できます。選択したしきい値を下回るWebサイトはブロックされます。このオプションは、ページの最初のオプションを*許可*に設定した場合に限り使用できます。Webサイトの評判について詳しくは、http://www.trustedsource.orgを参照してください。

*次へ*をクリックして次の設定ページに進み、*保存*をクリックして設定を保存するか、*キャンセル*をクリックしてすべての変更を破棄し、設定ダイアログを閉じます。

9.1.4.3 Webサイト

ブロックするWebサイト: #特定の URL や Web サイト、または特定のドメインにある複数の Web ページを、そのカテゴリに関わらずブロックするには、ここに入力します。その結果、ここで定義した Web サイトが、許可するカテゴリに属している場合でも、ブロックすることができます。

1. **「+」**アイコンをクリックして、*ホワイトリスト／ブラックリストオブジェクトの追加*ダイアログウィンドウを開きます。

2. **次の設定を行います。**
   - **名前**：ホワイトリスト/ブラックリストオブジェクトを説明する名前を入力します。
   - **次を基にURLと照合**：ドメイン1つまたは複数のドメイン名を入力します。*サブドメインを含める*にチェックを入れると、サブドメインも照合するようになります（example.comが、www.example.comおよびmail.example.comにも一致）。*サブドメインを含める*を選択しない場合、ドメイン名そのもののみが照合されます。
   - **次を基にURLと照合**：正規表現。URL全体に対して照合させるのに使用する正規表現を入力します。*以下のドメインに合致した場合のみ適用する*にチェックを入れると、正規表現適用前に照合させなければならないドメインのリストを指定できます。パスに対して照合させる必要がある場合、正規表現の使用が役に立ちます。

   クロスリファレンス – Webフィルタでの正規表現の使用に関する詳細情報は、SophosKnowledgebaseを参照してください。

   注 – エントリは正しい正規表現でなければなりません。例えば、*.example.comは有効ではありません。ドメイン名を照合させようと試みている場合、「.*」はパス内で拡張する可能性があるため、使わないでください。例えば、正規表現http://.*example¥.comは、http://www.google.com/search?www.example.comにも照合されます。

- コメント(オプション):説明などの情報を追加します。

3. *保存*をクリックします。

許可するWebサイト: 特定のURLまたはWebサイト、あるいは特定のドメインのウェブページのサブセットを、カテゴリを問わず許可したい場合には、ここで指定します。これにより、ここで指定されたWebサイトを、たとえブロックされるカテゴリに属していても許可することができるという効果があります。

1. 「**+**」アイコンをクリックして、*正規表現オブジェクトの追加*ダイアログウィンドウを開きます。

2. **次の設定を行います。**
   - **名前**:ホワイトリスト/ブラックリストオブジェクトを説明する名前を入力します。
   - **次を基にURLと照合**:ドメイン1つまたは複数のドメイン名を入力します。*サブドメインを含める*にチェックを入れると、サブドメインも照合するようになります(example.comが、www.example.comおよびmail.example.comにも一致)。*サブドメインを含める*を選択しない場合、ドメイン名そのもののみが照合されます。
   - **次を基にURLと照合**:正規表現。URL全体に対して照合させるのに使用する正規表現を入力します。*以下のドメインに合致した場合のみ適用する*にチェックを入れると、正規表現適用前に照合させなければならないドメインのリストを指定できます。パスに対して照合させる必要がある場合、正規表現の使用が役に立ちます。

     クロスリファレンス – Webフィルタでの正規表現の使用に関する詳細情報は、SophosKnowledgebaseを参照してください。

     注 – エントリは正しい正規表現でなければなりません。例えば、*.example.comは有効ではありません。ドメイン名を照合させようと試みている場合、「.*」はパス内で拡張する可能性があるため、使わないでください。例えば、正規表現http://.*example¥.comは、http://www.google.com/search?www.example.comにも照合されます。

   - コメント(オプション):説明などの情報を追加します。

3. *保存*をクリックします。

Webサイトリストでタグ付けされたコントロールサイト: 関連するタグがあるサイトについて、許可するか、ブロックするか、警告するか、利用可能な割当て時間に対してカウントするかを、制御できます。

1. *プラスアイコン*をクリックして、新規タグを追加します。または、*フォルダアイコン*をクリックして、既存のタグを選択します。
2. 各タグについて、*許可*、*警告*、*ブロック*、または*割当て*を選択します。
3. *保存*をクリックします。

9.1.4.4 ダウンロード

どのファイルタイプおよびMIMEタイプをブロックまたは警告するか設定します。

警告するファイル拡張子: ユーザが*警告するファイル拡張子*リスト内の拡張子を持つファイルのダウンロードを試みると、まず警告ページが表示されます。ファイル拡張子を追加するには、*警告するファイル拡張子*ボックスの「+」アイコンをクリックし、警告する拡張子(`exe`など)を入力します。ファイル拡張子に、先行するドットは含めないでください。

ブロックするファイル拡張子: ユーザが*ブロックするファイル拡張子*リスト内の拡張子を持つファイルのダウンロードを試みると、その試行はブロックされます。ファイル拡張子を追加するには、*ブロックするファイル拡張子*ボックスの「+」アイコンをクリックし、ブロックする拡張子(`exe`など)を入力します。ファイル拡張子に、先行するドットは含めないでください。

注 – アーカイブ内のファイル(例、`zip`ファイル)は、ブロックするファイルタイプ、ブロックする拡張子、ブロックするMIMEタイプではスキャンされません。こうしたアーカイブ内のファイルからネットワークを保護するには、zip、rar、などのアーカイブファイルタイプのブロックを検討してください。

警告するMIMEタイプ: ユーザが*警告するMIMEタイプ*リスト内に記載のMIMEタイプのファイルのダウンロードを試みると、まず警告ページが表示されます。MIMEタイプを追加するには*警告するMIMEタイプ*ボックスの「+」アイコンをクリックし、MIMEタイプを入力します。*警告するMIMEタイプ*リストでワイルドカード(*)が使えます。例、`audio/*`。

ブロックするMIMEタイプ: ユーザが*ブロックするMIMEタイプ*リスト内に記載のMIMEタイプのファイルのダウンロードを試みると、その試行はブロックされます。MIMEタイプを追加するには*ブロックするMIMEタイプ*ボックスの「+」アイコンをクリックし、MIMEタイプを入力します。*ブロックするMIMEタイプ*リストでワイルドカード(*)が使えます。例、`audio/*`。

ダウンロードのブロック制限: このオプションを指定すると、指定されたサイズ(MB単位)を超えるファイルのダウンロードを禁止します。

*次へ*をクリックして次の設定ページに進み、*保存*をクリックして設定を保存するか、*キャンセル*をクリックしてすべての変更を破棄し、設定ダイアログを閉じます。

9.1.4.5 ウイルス対策

フィルタアクション > *ウイルス対策*ページで、ウイルス対策用のWebフィルタ設定およびアクティブコンテンツの削除を設定可能です。

ウイルス対策

ウイルス対策スキャンを使用:このオプションを選択すると、受信および送信のWebトラフィックでウイルスをスキャンします。Sophos UTMは、さまざまなウイルス対策エンジンを備えています。

- シングルスキャン: デフォルト設定。*システム設定* > *スキャン設定*タブに定義されたエンジンを使用して最高レベルのパフォーマンスを実現します。
- デュアルスキャン:各トラフィックに対し、異なるウイルススキャナを使用してスキャンを2回行うことにより、検知率を最大限に高めます。デュアルスキャンは、ベーシックガードサブスクリプションでは使用できません。
- 望ましくないアプリケーション **PUA** をブロックする:PUAとは、悪意はないが、ビジネス環境に不適切な場合があるプログラムです。この機能を利用できるのは、Sophosアンチ・ウィルス・エンジンを使用するときだけです。特定のPUAを許可するには、ブロックが有効であれば、*Webフィルタリング* > *フィルタリングオプション* > *望ましくないアプリケーション*で例外を追加します。

次のサイズより大きいファイルはスキャンしない: ウイルス対策エンジンでスキャンする最大ファイルサイズを指定します。このサイズを超えるファイルはスキャン対象外となります。

> ヒント – 最大スキャンサイズより大きいファイルがダウンロードされることを防ぐには、*ダウンロード*ページで*ダウンロードのファイルサイズ制限*の値を設定します。

アクティブコンテンツ除去

*アクティブコンテンツ削除*エリアでは、Webページに埋め込まれたオブジェクトなど特定のWebコンテンツが自動的に削除されるように設定することができます。以下の設定が可能です。

- **JavaScript**の無効化:この機能はHTMLページ内のすべての`<SCRIPT>`タグを無効にするため、結果としてHTMLページに埋め込まれた機能やインクルードされた機能が無効になります。
- 埋め込みオブジェクトの削除 **ActiveX/Java/Flash** :この機能はすべての`<OBJECT>`タグをHTMLページから削除し、ActiveX、Flash、Javaなどの動的コンテンツを受信HTTPトラフィックから除去します。

*次へ*をクリックして次の設定ページに進み、*保存*をクリックして設定を保存するか、*キャンセル*をクリックしてすべての変更を破棄し、設定ダイアログを閉じます。

9.1.4.6 追加オプション

Webサイトプロテクション機能を強制する

セーフサーチ: 一部の検索プロバイダには、検索結果からアダルトコンテンツを除外するように設計されたセーフサーチ機能があります。Google、Bing、Yahooでセーフサーチの使用を強制することができます。有効にすると、プロバイダのセーフサーチが強制され、Webフィルタのユーザがオフにしたり、バイパスしたりすることはできません。この機能を設定するには、強制させたいセーフサーチを持つプロバイダを選択します。

YouTube for Schools: これを有効にすると、ユーザが再生できるYouTube動画は、YouTube EDUサブセクションのYouTube動画かユーザの学校のアカウントでアップロードされているYouTube動画に制限されます。これが機能するためには、YouTube for Schools プログラムに登録して、スクール ID を取得し、それを以下に入力する必要があります。

> 注 – Sophos UTMでは、トップレベルドメインの`youtube.com`と`ytimg.com`に加え、一般的な動画がブロックされないことを確認する必要があります。*YouTube for Schools*を有効にした場合、スクールID またはYouTubeから提供されたコードを入力する必要があります。

Google Appsの許可ドメインを強制する: Google Appsは、GoogleアカウントがGoogle Appsドメインのメンバでない限り、ユーザが特定のサービスからアクセスをすることをブロックできます。これをオンにするとこの機能が強制され、Webフィルタユーザがこれをオフにしたり、バイパスしたりすることはできません。この機能を設定するには、*Google Appsの許可ドメインを強制する*を選択します。次に、*ドメイン*ボックスの上部で、「+」アイコンまたはアクションアイコンをクリックして、Google Appsドメインを追加またはインポートします。

割当て

割当てに含まれるすべてのカテゴリやタグに許可される時間　分　オプションの時間を入力または変更します。

> 注 – *割当て*に設定されているすべてのサイトカテゴリおよびタグは、利用可能な割当て時間に対してカウントされます。利用可能な割当て時間は午前0時にリセットされます。または、*Webプロテクション > ポリシヘルプデスク > 割当てステータス*ページで手動でリセット可能です。

ネットワーク設定

親プロキシを、グローバルかプロファイルに基づいてかの両方で設定できます（*Webプロテクション > フィルタリングオプション > 親プロキシ*を参照）。

注 – 親プロキシを有効化した場合は、SSLスキャニングを有効にした状態での透過モードでのHTTPS要求は*行えません*。

親プロキシを設定するには、次の手順に従います。

1. **親プロキシリストの上部にあるプラス(+)アイコンをクリックします。**
   *親プロキシの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前：親プロキシを説明する名前を入力します。

   コメント(オプション)：説明などの情報を追加します。

   プロキシを使用するホスト：親プロキシを使用するホストをこのボックスに追加します(例：`*.wikipedia.org`)。ここではパターンマッチを使用できます。ただし、正規表現は使用できません。ボックスを空にすると、*保存*をクリックするとアスタリスク(*)が自動的に追加され、すべてのホストに該当します。従って、このようなプロキシ定義は、一致するプロキシが存在しない場合のフォールバックプロキシとみなされます。

   親プロキシ：親プロキシのネットワーク定義を選択または追加します。

   ポート：親プロキシ接続のデフォルトポートは8080です。親プロキシで別のポートを使用する場合、ここで変更できます。

   プロキシ認証が必要：親プロキシが認証を必要とする場合は、チェックボックスにチェックを入れ、表示されるテキストボックスにユーザー名とパスワードを入力します。

3. ***保存*をクリックします。**
   新しい親プロキシが*親プロキシ*リストおよび*Webプロテクション > フィルタリングオプション > 親プロキシ*ページに表示されます。

親プロキシを編集または削除するには、プロキシの名前をクリックします。

アクティビティ記録

どのアクティビティを記録するかを選択できます。

- アクセスしたページのログ：この機能は、UTMを通じてアクセスされたすべてのページに関する情報を記録します。

- ブロックしたページのログ：この機能は、アクセスがブロックされたページに関する情報を記録します。

*保存*をクリックして設定を保存するか、*キャンセル*をクリックしてすべての変更を破棄して、設定ダイアログを閉じます。

9.2 Webフィルタプロファイル

フィルタプロファイルを使用すると、複数のコンテンツフィルタリングポリシを作成し、ネットワーク内のさまざまなアドレスに別々のポリシを適用することができます。社内の各ネットワークに同じポリシを適用する場合、*Webプロテクション > Webフィルタリング*でこれを行えます。さらに、各フィルタプロファイルには独自のユーザ認証方式を設定できます。

複数のフィルタプロファイルを利用して、異なるネットワークの認証およびWebコンテンツを制御できます。例えば、AD SSOを使用する会社のコンピュータ向けポリシを設定できますし、異なる認証方式およびゲストワイヤレスネットワークのポリシを用意することもできます。

9.2.1 フィルタプロファイル

複数のネットワークに異なるポリシまたは認証モードを適用する場合、複数のフィルタプロファイルを作成可能です。例えば、有線ネットワークでAD搭載の会社のコンピュータのみが認められている場合、したがって明示プロキシおよびAD SSOによる標準モードを使用することになります。ワイヤレスネットワークには、従業員がAD資格情報入力するブラウザログインポータルや、アクセスを制限するゲストログイン機能があるかもしれません。

プロファイルは、*Webフィルタプロファイル > フィルタプロファイル*タブで作成できます。Web要求が行われると、UTMはソースIPを閲覧して、一致する*許可ネットワーク*と*オペレーションモード*を持つ最初のプロファイルを適用します。*デフォルトのWebフィルタプロファイル*は、*Webプロテクション > Webフィルタリング*ページで設定されます。ここにリストされているのは、当該フィルタプロファイルが最後に一致するプロファイルであることを示すためです。プロファイルが選択されると、UTMはそのプロファイルにしたがって認証およびポリシを実行します。

フィルタプロファイルを作成するには：

1. **右上のプラス(+)アイコンをクリックします。**
   *プロファイルの追加*ウィザードが開きます。

2. *名前*と*コメント*を入力します。

3. **許可するネットワークを選択します。**

Webフィルタの使用を許可するネットワークを選択します。デフォルトで、Webフィルタはクライアント要求をTCPポート8080でリスンし、*許可ネットワーク*ボックスにリストされたネットワーク内のすべてのクライアントに対して接続を許可します。

4. **許可されるエンドポイントグループを選択します。**
エンドポイントWebコントロールが有効であれば、Webフィルタの使用を許可するエンドポイントグループを選択します

5. **HTTPS(SSL)トラフィックのオプションを選択する。**
SSLトラフィックのスキャンは次のオプションから選択:

- *スキャンしない*:このオプションは、透過モードのみで使用可能です。選択した場合、HTTPSトラフィックはプロキシを経由せず、スキャンは実施されません。
- **URL** *フィルタリングのみ*:このオプションは、URLカテゴリおよび評判チェックが実行されますが、HTTPSトラフィックのコンテンツのスキャンは実施されません。
- *複合化およびスキャン*:このオプションを選択した場合、HTTPSトラフィックの複合化および完全チェックが実行されます。

6. **オペレーションのモードを選択します。**
ユーザ認証が必要なオペレーションモードを選択する場合には、Webフィルタの使用を許可するユーザとグループを選択する必要があります。次のオペレーションモードを使用できます。

- 標準:標準モードでは、Webフィルタはデフォルトでクライアント要求をポート8080でリスンし、*送信元ネットワーク*ボックスにリストされたネットワーク内のすべてのクライアントに対して接続を許可します。このモードで使用する場合、クライアントはブラウザの設定でWebフィルタにHTTPプロキシを指定していることが必要です。

  *デフォルト*の認証モードを選択します。

  - なし:認証をしない場合に選択します。
  - **Active Directory SSO**:このモードでは、コンピュータにプロキシのユーザとして現在ログインしている(シングルサインオン)ユーザの認証が試行されます。現在ログインしているユーザがプロキシ使用許可を持つ有効なADユーザである場合、認証はユーザインタラクションなしで行われるはずです。*定義とユーザ* > *認証サービス* > *サーバ*タブで、*Active Directory*シングルサインオン *Active Directory Single Sign-On* (SSO)が設定されていなければなりません。クライアントはNTLMまたはKerberosで認証可能です。

- エージェント: SophosAuthentication Agent（SAA）を使用する場合に選択します。Webフィルタを使用するためには、エージェントと認証を開始する必要があります。エージェントは、ユーザポータルからダウンロードできます。ユーザポータルをご覧ください。
- **Apple OpenDirectory SSO**: *定義とユーザ* > *認証サービス* > *サーバタブでLDAP*を設定しており、Apple OpenDirectoryを使用している場合、これを選択します。さらに、プロキシが正しく機能するようにするためには、*Webプロテクション* > *フィルタリングオプション* > *その他*タブで、MAC OS Xシングルサインオン Kerberos鍵ファイルをアップロードする必要があります。このモードで使用する場合、クライアントはブラウザの設定でWebフィルタにHTTPプロキシを指定していることが必要です。SafariブラウザはSSOをサポートしていません。
- 基本ユーザ認証：このモードでは、各クライアントはプロキシを使用する前にこのプロキシに対して自己認証する必要があります。サポートされる認証方式について詳しくは、*定義とユーザ* > *認証サービス*を参照してください。このモードで使用する場合、クライアントはブラウザの設定でWebフィルタにHTTPプロキシを指定していることが必要です。
- ブラウザ：選択すると、Webフィルタへの自己認証のためのログインダイアログがユーザのブラウザに表示されます。このモードでは、クライアント側のブラウザ設定なしで、ユーザ名に基づく追跡、報告、およびサーフィンが可能になります。さらに、そのダイアログウィンドウに追加で免責条項を表示することができます。この場合、ユーザが先に進むためには、免責条項に同意する必要があります。免責条項について詳しくは、*マネジメント* > *カスタマイズ* > *Webメッセージ*の章を参照してください。
- **eDirectory SSO**: *定義とユーザ* > *認証サービス* > *サーバ*タブで*eDirectory*を設定した場合、これを選択します。

> 注 – eDirectoryのシングルサインオン（SSO）モードの場合、WebフィルタはアクセスY先のIPアドレスと資格情報を最大15分間キャッシュします。Apple OpenDirectory SSOの場合、キャッシュできるのはグループ情報のみです。これは、認証サーバへの負荷を軽減するために行われます。逆に言うと、ユーザ、グループ、またはアクセスしているユーザのログインステータスの変更がWebフィルタによって反映されるまで、最大15分かかります。

ユーザ認証が必要な認証モードを選択した場合は、*認証失敗のアクセスをブロック*を選択し、認証を失敗したユーザのアクセスを拒否します。

- 透過モード: 透過モードでは、ポート80(SSLを使用している場合はポート443)でクライアントブラウザアプリケーションが行うすべての接続はインターセプトされ、クライアント側の設定なしでWebフィルタにリダイレクトされます。クライアントがWebフィルタサーバを意識することは全くありません。このモードのメリットは、多くのインストールについては、その他の管理やクライアント側の設定が必要ないということです。しかし、処理可能なのはHTTP要求のみという短所があります。そのため、透過モードを選択すると、クライアントのプロキシ設定は無効になります。

> 注 – 透過モードでは、WebフィルタはHTTP要求からNTLM認証ヘッダを削除します。さらに、WebフィルタはこのモードではFTP要求を処理できません。クライアントがこのようなサービスにアクセスする必要がある場合は、ファイアウォールでポート(21)を開く必要があります。一部のWebサーバは、ポート80以外のポート経由でストリーミング動画や音声などのデータを送信します。これらの要求は、Webフィルタが透過モードで機能しているときは検知されません。このようなトラフィックにも対応したい場合には、他のモードを使用するか、これらを許可する明確なファイアウォールルールを入力する必要があります。

  - なし: 認証をしない場合に選択します。
  - **Active Directory SSO**: このモードでは、コンピュータにプロキシのユーザとして現在ログインしている(シングルサインオン)ユーザの認証が試行されます。現在ログインしているユーザがプロキシ使用許可を持つ有効なADユーザである場合、認証はユーザインタラクションなしで行われるはずです。*定義とユーザ* > *認証サービス* > *サーバ*タブで*Active Directoryシングルサインオン SSO* を設定する必要があります。クライアントは、NTLM(またはMacの場合はKerberos)を使用して認証を行えます。一部の環境については、エンドポイントの追加設定が必要です。透過モードでSSOに関する問題がある場合、Sophos Knowledgebase Article 120791をご覧ください。

    > 注 – Active Directoryユーザグループを定義する場合、LDAP文字列の代わりにプレーンなActive Directoryのグループまたはユーザの名前を手動で入力することで、*Active Directoryグループ*ボックスに必要なエントリを追加することを強く推奨いたします。例: LDAP文字列CN=ads_group1,CN=Users,DC=example,DC=comの代わりに、単に名前ads_group1を入力します。

> **注** – Kerberosを使用している場合は、ユーザを入力することをWebフィルタが許可していないので、単にグループを*Active Directoryグループ*ボックスに追加するだけです。

- エージェント: SophosAuthentication Agent(SAA)を使用する場合に選択します。Webフィルタを使用するためには、エージェントと認証を開始する必要があります。
- ブラウザ: 選択すると、Webフィルタへの自己認証のためのログインダイアログがユーザのブラウザに表示されます。このモードでは、クライアント側のブラウザ設定なしで、ユーザ名に基づく追跡、報告、およびサーフィンが可能になります。さらに、そのダイアログウィンドウに追加で免責条項を表示することができます。この場合、ユーザが先に進むためには、免責条項に同意する必要があります。免責条項について詳しくは、*マネジメント > カスタマイズ > Web メッセージ*の章を参照してください。

- フル透過 (オプション):クライアントの送信元IPをゲートウェイのIPに置き換えず、そのまま維持する場合は、選択します。これは、クライアントがパブリックIPアドレスを使用しており、Webフィルタによって隠すべきではない場合に便利です。このオプションはブリッジモードでの実行中においてのみ利用可能です。

  *フル透過*で利用可能な認証モードは、*透過*と同じです。上記をご覧ください。

認証の使用を設定する場合、*認証失敗のアクセスをブロック*するオプションがあります。AD SSOを使用中で認証失敗のアクセスをブロックしない場合、SSOの認証失敗により、ユーザプロンプトなしで未認証のアクセスが許可されてしまいます。ブラウザ認証を使用中で認証失敗のアクセスをブロックしない場合、ログインページに追加の*ゲストログイン*リンクが現れ、未認証のアクセスが許可されます。

7. **デバイス固有の認証を有効にする。**
   特定のデバイスの認証モードを設定するには、*デバイス固有の認証を有効にする*チェックボックスを選択します。有効になると、緑の「+」アイコンをクリックして、デバイスのタイプや関連する認証モードを追加することができます。

8. ***次へ*をクリックするか、ウィザードの上部から*ポリシ*を選択します。**

9. **レビューして、フィルタプロファイルのポリシを作成します。**
   新しいポリシを作成するには、以下の手順に従います。

   1. **右上のプラス(+)アイコンをクリックします。**
      *ポリシの追加*ダイアログボックスが表示されます。

2. **次の設定を行います。**
名前:このポリシを説明する名前を入力します。

ユーザ/グループ:このポリシを適用させるユーザまたはユーザグループを選択します。また、新しいユーザまたはグループの作成もできます。ユーザを追加する方法は、*定義とユーザ* > *ユーザとグループ* > *ユーザ*ページで説明しています。

時刻イベント:ポリシは、選択した期間の間有効になります。ポリシを常に有効にしておくには、*Always*を選択します。また、緑色の「+」アイコンをクリックして、新しい時刻イベントを作成することもできます。期間定義は、*定義とユーザ* > *期間定義*タブで管理します。

フィルタアクション:既存のフィルタアクションを選択します。これにより、ポリシに適用させるWebプロテクションのタイプが定義されます。また緑色の「+」アイコンをクリックし、*フィルタアクションウィザード*を使用して新規フィルタアクションを作成することもできます。フィルタアクションも、*Web フィルタプロファイル* > *フィルタアクション*タブで管理できます。

コメント(オプション):説明などの情報を追加します。

詳細設定:

- 例外のため認証を省略したリクエストにポリシを適用する: *フィルタリングオプション* > *除外*タブで、例えば、認証を使用できない自動アップロードでの認証を省略するための例外を作成できます。このポリシを認証を省略したWebリクエストに適用する場合は、このチェックボックスを選択します。

3. ***保存*をクリックします。**
新しいポリシが*ポリシ*リストに表示されます。

4. **ポリシを有効にします。**
新規ポリシは、デフォルトで無効になっています(トグルスイッチは灰色)。ポリシを有効にするには、トグルスイッチをクリックします。これでポリシが有効になります(トグルスイッチは緑)。

10. ***保存*をクリックします。**
新しいプロファイルが*フィルタプロファイル*リストに表示されます。

重要 – SSL スキャニングを透過モードと組み合わせて有効にすると、一部の SSL 接続(SSL VPNトンネルなど)が失敗します。SSL VPN接続を有効にするには、対応するターゲットホストを*透過モードスキップリスト*に追加します(*Webプロテクション* > *フィルタリングオプション* > *その他*を参照)。さらに、自己署名証明書でホストにアクセスするには、*証明書信頼性チェック*オプションを

選択して、これらのホストの除外を作成する必要があります。これにより、プロキシで証明書のチェックが行われません。

フィルタプロファイルを編集または削除するには、リストでプロファイルの名前をクリックします。

9.2.2 フィルタアクション

*Web フィルタリングプロファイル > フィルタアクション*タブでは、一連のWebプロテクション構成設定を作成および編集できます。この設定を使用して、さまざまなタイプやレベルの保護をカスタマイズすることが可能です。フィルタアクションは、さまざまなユーザやユーザグループに割り当てることができ、Webアクセスをコントロールするための柔軟な手法となります。

*新規フィルタアクション*ボタンをクリックし、新しいフィルタアクションを作成、または対応する*編集*ボタンをクリックし、既存のフィルタアクションを編集することができます。どちらのアクションに対してもフィルタアクションウィザードが起動します。詳しくは、*Webプロテクション > ポリシ > フィルタアクションウィザード*を参照してください。

*フィルタアクション*ページで、既存のフィルタアクションのリストの検索、複製、削除または閲覧を行うこともできます。

9.2.3 親プロキシ

一部のネットワークトポロジーでは、アップストリームのWebプロキシサーバが必要です。*Webプロテクション > Web フィルタプロファイル > 親プロキシ*ページで、親プロキシを設定できます。

親プロキシを設定するには、次の手順に従います。

1. ***新規親プロキシ*をクリックします。**
   *親プロキシの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前：この親プロキシを説明する名前を入力してください。

   コメント(オプション)：説明などの情報を追加します。

   プロキシを使用するホスト：親プロキシを使用するホストをこのボックスに追加します(例：`*.wikipedia.org`)。ここではパターンマッチを使用できます。ただし、正規表現は使用できません。ボックスを空にすると、*保存*をクリックするとアスタリスク(*)が自動的に追

加され、すべてのホストに該当します。従って、このようなプロキシ定義は、一致するプロキシが存在しない場合のフォールバックプロキシとみなされます。

親プロキシ：親プロキシのネットワーク定義を選択または追加します。

ポート：親プロキシ接続のデフォルトポートは8080です。親プロキシで別のポートを使用する場合、ここで変更できます。

プロキシ認証が必要：親プロキシが認証を必要とする場合は、チェックボックスにチェックを入れ、表示されるテキストボックスにユーザー名とパスワードを入力します。

3. ***保存*をクリックします。**
   新しい親プロキシが*親プロキシ*リストに表示されます。

これで、このプロキシをフィルタアクションで使用することも、グローバルに使用することもできます。

親プロキシを編集または削除するには、対応するボタンをクリックします。

9.3 フィルタリングオプション

*Webプロテクション > フィルタリングオプション*ページで、Webフィルタリングのさまざまなオプションを設定できます。このページからアクセスできるタブで、フィルタリングの除外、フィルタリングをバイパスできるユーザ、フィルタリングのカテゴリ、HTTPS証明書や認証局、さらに多くのさまざまなオプションを設定できます。

9.3.1 除外

*Webプロテクション > フィルタリングオプション > 除外*タブでは、クライアントネットワーク、ユーザ/グループ、ドメインのホワイトリストを定義できます。これらのリストに含まれるすべてのエントリを、特定のWebプロテクションサービスの対象外にすることができます。

除外ルールを作成するには、次の手順に従います。

1. ***除外*タブで、*新規除外リスト*をクリックします。**
   *除外リストを追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前：この除外ルールを説明する名前を入力してください。

   コメント（オプション）：説明などの情報を追加します。

   スキップするチェック：スキップするセキュリティチェックを選択します。

- 認証：Webフィルタを*認証*モードで実行している場合、送信元ホスト/ネットワークまたはターゲットドメインの認証をスキップできます。
- *キャッシング*：選択すると、特定のドメインまたは送信元ホスト/ネットワークのキャッシングが無効になります。
- *ダウンロードサイズでブロック*：選択すると、ダウンロードのサイズに従ってコンテンツのブロックを無効にします。
- *ウイルス対策*：選択すると、ウイルスやトロイの木馬などの好ましくないコンテンツがメッセージに含まれていないかチェックするウイルススキャンが無効になります。
- 拡張子*ブロック*：選択すると、ファイル拡張子フィルタが無効になります。このフィルタは、拡張子に基づいて特定タイプのファイルが含まれるコンテンツをブロックするために使用します。
- **MIME***タイプブロック*：選択すると、MIMEタイプフィルタが無効になります。このフィルタは、特定のMIMEタイプのコンテンツをブロックするために使用します。
- **URL***フィルタ*：選択すると、URLフィルタが無効になります。このフィルタは、特定の種類のWebサイトへのアクセスをコントロールします。
- *コンテンツ*削除：選択すると、（マルチメディアファイルなどの）埋め込みオブジェクトやJavaScriptといったWebページ内の特殊コンテンツの削除がバイパスされます。
- **SSL***スキャン*：選択すると、要求内のWebページに対するSSLスキャンがスキップされます。これは、オンラインバンキングのWebサイトや、SSLインターセプションがうまく機能しないWebサイトなどで有用です。技術的な理由から、このオプションは透過Webフィルタモードでは機能しません。透過モードでは、代わりに*透過モードスキップリスト*を使用してください（*フィルタオプション > その他*タブを参照）。標準モードでは、クライアントが何を送信するのかに応じて、宛先ホストまたはIPアドレスのみに基づいて除外を行うことができます。URL全体ではなくカテゴリに基づく除外では、ホスト名のみが分類されます。
- 証明書信頼性*チェック*：選択すると、HTTPSサーバ証明書の信頼性チェックがスキップされます。Webフィルタが認証ありの透過モードで機能している場合、ユーザ/グループの照合に基づく証明書の信頼性チェックをスキップすることは技術的に不可能です（*ユーザ/グループからの全リクエストに適用*）。
- 証明書日付*チェック*：選択すると、HTTPS証明書の日付が有効であるかどうかのチェックがスキップされます。

アクティビティをログすべきではない人がいる場合には、次の2つのオプションが便利です。

- アクセスしたページ：選択すると、アクセスしたページのログが記録されなくなります。これらのページ要求は、レポートからも除外されます。
- ブロックしたページ：選択すると、ブロックされたページのログが記録されなくなります。これらのページ要求は、レポートからも除外されます。

一部のソフトウェアアップデートおよび類似のダウンロードは、進行状況ページが表示されると中断される場合があります。ソフトウェアアップデートで問題がある場合、またはあるダウンロードがいつまでも完了しない場合は、以下のオプションを選択します。

- ダウンロード/検索の進行状況ページを表示しない：これを選択すると、ダウンロードおよびスキャンの進行状況ページが無効となります。

対象：セキュリティチェックをスキップする条件を少なくとも1つ選択します。条件の前にあるドロップダウンリストで*And*または*Or*を選択して、複数の条件を論理的に組み合わせることができます。次の条件を設定できます。

- 送信元ホスト/ネットワークで除外：選択して、この除外ルールのセキュリティチェックから除外する送信元ホスト/ネットワークを追加します。条件を選択すると、*ホスト/ネットワーク*ボックスが開くので、各ホストまたはネットワークを入力します。
- 送信元エンドポイントグループで除外：選択して、この除外ルールのセキュリティチェックから除外するコンピュータグループを追加します（*エンドポイントプロテクション* > *コンピュータ管理* > *グループ管理*タブを参照）。条件を選択すると*送信元エンドポイントグループ*ボックスが開くので、各グループを入力します。
- これらの**URL**と照合：選択して、この除外ルールのセキュリティチェックから除外するターゲットドメインを追加します。条件を選択すると*ターゲットドメイン*ボックスが開くので、各ドメインを追加します。ここでは、正規表現を使用することができます。例：`^https?://[^.]*\.domain.com`は、ドメインのすべてのサブドメインへのHTTP（S）接続と一致します。

  クロスリファレンス – Webフィルタでの正規表現の使用に関する詳細情報は、SophosKnowledgebaseを参照してください。

  注 – SSLスキャニングを有効にして*透過*モードを使用している場合、ターゲットドメインをIPアドレスで入力する必要があります。IPアドレスを入力しないと、除外は技術的な理由で失敗します。

- 送信元ユーザ/グループ：選択して、この除外ルールのセキュリティチェックから除外するユーザまたはユーザグループを追加します。条件を選択すると*ユーザー/グルー*

プボックスが開くので、各ユーザーまたはグループを入力します。また、標準モードでは認証が存在しないため、特定のユーザ/グループの照合は機能しません。

- **宛先Web**サイトカテゴリ: 選択すると、特定のカテゴリに対するセキュリティチェックがスキップされます。条件を選択するとリストが開くので、カテゴリを選択します。
- 送信元ユーザエージェント: これを選択すると、ユーザエージェント文字列によるウリクエストのセキュリティチェックが省略されます。正規表現を使用することができます。

3. ***保存*をクリックします。**
   新しい除外ルールが*除外*リストに表示されます。

除外ルールを編集または削除するには、対応するボタンをクリックします。

9.3.2 Webサイト

Webプロテクション > *フィルタリングオプション* > *Webサイト*タブでは、デフォルトのカテゴリや評判を上書きしたいサイトのリストを管理できます。または、タグをサイトに関連付けできます。

*ローカルサイトリスト*にエントリを追加するには:

1. ***サイトを追加*ボタンをクリックします。**
2. **上書きしたいサイトまたはタグを入力します。**
   *ローカルサイトを追加*ダイアログのテキストボックスで、URL、ドメイン、IPアドレス、CIDR範囲を入力できます。
3. **オプションとして、*サブドメインを含める*チェックボックスを選択します。**
   このチェックボックスを選択すると、上書きがすべてのサブドメインに適用されます。たとえば、example.comを追加して、*サブドメインを含める*チェックボックスを選択すると、mail.example.comも上書き対象に含まれます。
4. **上書きする*カテゴリ*または*評判*を選択します。**
   カテゴリ、*評判*、あるいは両方を上書きできます。*ローカルサイトリスト*で定義したサイトは、こうした上書きの値を使用するフィルタアクションで処理されます。
5. **サイトに関連付ける*タグ*を選択します。**
   *プラス*アイコンをクリックして、新しいタグを作成します。または、*フォルダ*アイコンをクリックして既存のタグを選択します。タグ付けされたサイトは、タグを参照するフィルタアクションを作成して制御可能です。
6. **オプションとして、コメントを追加します。**

サイトのリストが大きい場合、タブの上部にある*次へ*や*前へ*のアイコンを使用してページ単位で移動したり、検索テキストボックスを使ってアイテムを検索したりすることができます。エントリを削除するには、エントリの横にある削除アイコンをクリックするか、複数のアイテムを選択して、リストの上部にある*削除*アイコンをクリックします。

9.3.3 バイパスユーザ

*Webプロテクション > フィルタリングオプション > バイパスユーザ*タブでは、ブロックページのバイパスが許可されるユーザを指定できます。

既存のグループまたはユーザを追加するには:

1. ***ブロックのバイパスが許可されるユーザ/グループ*の横にあるフォルダアイコンをクリックします。**
   左のナビゲーションペインに、既存のユーザおよびグループのリストが表示されます。

2. **ユーザまたはグループを選択して、*ブロックのバイパスが許可されるユーザ/グループ*ボックスにドラッグします。**
   これで、アイテムは*バイパスユーザ*タブにリストされます。

新しいユーザを追加するには:

1. ***ブロックのバイパスが許可されるユーザ/グループ*の横にある緑色の「+」アイコンをクリックします。**
   *ユーザの追加*ダイアログウィンドウが表示されます。

2. ***ユーザの追加*ダイアログウィンドウにユーザー情報を入力します。**
   ユーザを追加する方法は、*定義とユーザ > ユーザとグループ > ユーザ*ページで説明しています。

3. ***適用*をクリックします。**
   設定が保存されます。

9.3.4 望ましくないアプリケーション

*Webプロテクション > フィルタリングオプション > PUA*タブで、承認された望ましくないアプリケーション(PUA)のリストを管理できます。UTMは、ビジネス環境に望ましくないアプリケーションを識別し、それらをブロックすることができます。ブロックが有効になっている際に特定のPUAを許可するには、ブロックページまたはログで報告されたとしてその名を追加します。

*ローカルサイトリスト*にエントリを追加するには:

1. ***承認済みPUA*リストの「+」アイコンをクリックします。**
2. **PUA定義を入力します。**
   PUA定義を検索するには、*ログとレポート* > *Webプロテクション* > *Web使用状況レポート*と移動して、*利用可能なレポート*ドロップダウンから*PUA Downloader*を選択します。
3. ***適用*をクリックします。**

緑色の「+」アイコンの横にある*開くアクション*メニューアイコンをクリックすると、PUAのテキストリストのインポートやアウトポートおよび*承認済みPUA*リストのクリアなどができます。

9.3.5 カテゴリ

Webプロテクション > *フィルタリングオプション* > *カテゴリ*タブでは、Webサイトカテゴリのカテゴリグループへのマッピングをカスタマイズできます。これは*フィルタリングアクション*タブまたは*Webサイトフィルタリング*ページで選択できます。Sophos UTMは、異なるWebサイトカテゴリを識別し、アクセスをブロックすることができます。高度なURL分類方法により、疑わしいWebサイトの識別における精度と完全性が保証されます。データベースに含まれていないWebページをユーザが要求すると、URLがWebクローラに送信され、自動的に分類されます。

注 – Webサイトが正しく分類されていないと思われる場合は、次のURLレポートフォームを使用して新しいカテゴリをご提案いただけます。

Webサイトカテゴリをカテゴリグループに割り当てるには、次の手順に従ってください。

1. **編集するカテゴリグループで*編集*をクリックします。**
   *フィルタカテゴリの編集*ダイアログボックスが開きます。
2. **サブカテゴリを選択します。**
   グループに追加（またはグループから削除）するサブカテゴリのチェックボックスにチェックを入れます（またはチェックを外します）。
3. ***保存*をクリックします。**
   指定した設定でグループが更新されます。

あるいは、新しいフィルタカテゴリを作成することもできます。次の手順で実行します。

1. **ページ上部にある*新規フィルタカテゴリ*ボタンをクリックします。**
   *フィルタカテゴリの追加*ダイアログボックスが開きます。
2. **名前を入力します。**
   新しいフィルタカテゴリを説明する名前を入力してください。

3. **サブカテゴリを選択します。**
   グループに追加するサブカテゴリのチェックボックスを選択します。

4. ***保存*をクリックします。**
   指定した設定でグループが更新されます。

カテゴリを編集または削除するには、対応するボタンをクリックします。

9.3.6 HTTP/S CA

Webプロテクション > *Webフィルタリング* > *HTTPS CA*タブでは、HTTPS接続の署名および検証CA（認証局）を管理できます。

署名CA

このエリアでは、署名CA証明書のアップロード、署名CA証明書の再生成、または既存の署名CA証明書のダウンロードが可能です。デフォルトで署名CA証明書は、セットアップ中に提供された情報に基づいて作成されます。つまり、セットアップ後に何らかの変更が行われた場合を除き、*マネジメント* > *システム設定* > *組織*タブの情報と整合性があります。

新しい署名CA証明書をアップロードするには、次の手順に従ってください。

1. ***アップロード*ボタンをクリックします。**
   *PKCS#12証明書ファイルのアップロード*ダイアログウィンドウが開きます。

2. **アップロードする証明書までブラウズします。**
   *ファイル*ボックスの横にあるフォルダアイコンをクリックし、*ファイルのアップロード*ダイアログボックスが開いたら*参照*をクリックしてアップロードする証明書を選択し、*アップロード開始*をクリックします。

   パスワードで保護されているPKCS#12形式の証明書のみをアップロードできます。

3. **パスワードを入力します。**
   該当フィールドにパスワードをもう一度入力し、*保存*をクリックします。

   新しい署名CA証明書がインストールされます。

署名CA証明書を再生成するには、次の手順に従ってください。

1. ***再生成*ボタンをクリックします。**
   *新規署名CAの作成*ダイアログボックスが開きます。

2. **情報を変更します。**
   必要に応じて所定の情報を変更し、*保存*をクリックします。

新しい署名CA証明書が生成されます。これに基づき、*署名CA*エリア内の署名CA情報が変化します。

署名CA証明書をダウンロードするには、次の手順に従ってください。

1. ***ダウンロード*ボタンをクリックします。**
*証明書ファイルのダウンロード*ダイアログウィンドウが開きます。

2. **ダウンロードするファイル形式を選択します。**
2種類の形式から選択できます。

   - **PKCS#12**: この形式は暗号化されるため、エクスポートパスワードを入力してください。
   - **PEM**: 暗号化されない形式です。

3. ***ダウンロード*をクリックします。**
ファイルがダウンロードされます。

カスタムCAで署名された証明書を内部Webサーバに対して使用する場合、信頼される認証局としてこのCA証明書をWebAdminにアップロードすることをお勧めします。これを行わないと、Webフィルタが、信頼できないサーバ証明書が検知されたというエラーメッセージをユーザに表示します。

クライアントPCへのプロキシCA証明書の提供を円滑化するために、ユーザは自分でhttp://passthrough.fw-notify.net/cacert.pemから証明書をダウンロードし、ブラウザにインストールすることができます。Webサイト要求はプロキシで直接受信され、処理されます。そのため、まず*Webセキュリティ* > *グローバル*タブでWebフィルタを有効にする必要があります。

注 – プロキシのオペレーションモードが*透過モード*ではない場合、ユーザのブラウザでプロキシを有効にする必要があります。有効にしないと、証明書ダウンロード用のリンクがアクセス不可になります。

あるいは、ユーザポータルが有効であれば、ユーザはプロキシCA証明書をユーザポータルの*HTTPSプロキシ*タブからダウンロードできます。

HTTPSでの問題を回避する

HTTPSの使用中、Windows UpdateやWindows DefenderなどのWindowsシステムプログラムは接続を確立できません。これは、これらのプログラムが*システムユーザ*権限で実行されるためです。このユーザはデフォルトで、プロキシCAを信頼しないことになっています。そのため、システムユーザ用にHTTPSプロキシCA証明書をインポートする必要があります。以下の手順に従ってください。

1. **Windowsで、*Microsoft管理コンソール* mmc を開きます。**
2. ***ファイル*メニューをクリックし、*スナップインの追加と削除*をクリックします。**
   *スナップインの追加と削除*ダイアログウィンドウが開きます。
3. **ウィンドウの一番下にある*追加*をクリックします。**
   *スタンドアロンスナップインの追加*ダイアログウィンドウが開きます。
4. **リストから*証明書*を選択し、*追加*をクリックします。**
   ウィザードが表示されます。
5. *コンピュータアカウント*を選択し、*次へ*をクリックします。
6. ***ローカルコンピュータ*が選択されていることを確認し、*完了*、次に*閉じる*をクリックします。**
   最初のダイアログウィンドウに*証明書 ローカルコンピュータ* が追加されています。
7. ***OK*をクリックします。**
   ダイアログウィンドウが閉じて、コンソールルートに*証明書 ローカルコンピュータ* が追加されています。
8. **左側の *コンソールルート*ウィンドウで*証明書* > *信頼されたルート証明機関*を開き、*証明書*を右クリックして、コンテキストメニューの *すべてのタスク* > *インポート*を選択します。**
   インポートダイアログウィザードが開きます。
9. ***次へ*をクリックします。**
   次のウィザードステップが表示されます。
10. **以前にダウンロードしたHTTPSプロキシCA証明書までブラウズし、*開く*>*次へ*をクリックします。**
    次のウィザードステップが表示されます。
11. ***証明書をすべて次のストアに配置する*が選択されていることを確認し、*次へ*および*閉じる*をクリックします。**
    インポートの成功がウィザードから報告されます。
12. **ウィザードのメッセージを確認します。**
    信頼される証明書の中に、プロキシCA証明書が表示されるようになりました。
13. **変更を保存します。**
    *ファイル*メニューをクリックし、*保存*をクリックして、コンソールルートでの変更を保存します。

インポート後、CAはシステム全体で受け入れられるようになり、HTTPSプロキシに起因する接続問題は発生しなくなります。

検証CA

このエリアでは検証CAを管理できます。検証CAとは、最初に信頼する認証局です。つまり、これらのCAによって署名された有効な証明書を提示するWebサイトは、HTTPプロキシによって信頼できると見なされます。

ローカル検証**CA**: 下のCAリストに追加して検証CAをアップロードできます。次の手順で実行します。

1. ***ローカルCAのアップロード*フィールドの横のフォルダアイコンをクリックします。**
   *ファイルのアップロード*ダイアログウィンドウが開きます。

2. **アップロードする証明書を選択します。**
   *参照*をクリックして、アップロードするCA証明書を選択します。PEMの証明書の拡張子のみがサポートされています。

3. **証明書をアップロードします。**
   *アップロード開始*をクリックして、選択したCA証明書をアップロードします。

   証明書はインストールされ、*ローカル検証CA*エリアに表示されます。

グローバル検証**CA**: ここに表示される検証CAのリストは、Mozilla Firefoxにあらかじめインストールされた検証CAと同じです。ただし、リストに含まれるいずれか(あるいは全部)の検証CAを「信頼できない」場合は、これらを無効にすることができます。CAの証明書を無効にするには、トグルスイッチをクリックします。トグルスイッチがグレーになり、HTTPSプロキシはこのCAによって署名されたWebサイトを受け入れなくなります。

ヒント – CA の指紋を表示するには、青色の情報アイコンをクリックしてください。

CAが不明または無効である場合、HTTPSプロキシはクライアントに対して「ブロックされたコンテンツ」のエラーページを表示します。However, you can create an exception for such pages: either via the *Create Exception* link on the error page of the Web Filter or via the *Web Protection* > *Filtering Options* > *Exceptions* tab.

注 –Webフィルタのエラーページで*除外の作成*リンクをクリックすると、ログインダイアログウィンドウが表示されます。admin権限のあるユーザのみが除外を作成できます。

9.3.7 その他

*Webプロテクション > フィルタリングオプション > その他*タブには、キャッシングやポートの設定など、Webフィルタの各種設定オプションが用意されています。

その他 の設 定

Web フィルタリングポート: ここで、Webフィルタがクライアントのリクエストに対して使用するポート番号を定義できます。デフォルトは8080です。

注 – これが適用されるのは、プロキシを透過モードで操作していない場合のみです。

HTTPループバックの検出 : このオプションはデフォルトで有効になっています。HTTPループバックの検出の無効化は、UTMがオリジナルの宛先でありポートが80であるDNATルールがある場合にのみ行ってください。

MIMEブロックによる**HTTP**ボディの検査 : HTTPヘッダのみならず、HTTPボディも、ブロック対象MIMEタイプに対してチェックされます。この機能をオンにすると、パフォーマンスが低下する可能性があります。

スキャンできないファイル、暗号化されたファイルのブロック: スキャンできないファイルをブロックするには、このオプションを選択します。スキャンできない理由はいくつかありますが、ファイルが暗号化されているか、破損している可能性があります。

許可されるターゲットサービス: *許可されるターゲットサービス*ボックスでは、Webフィルタのアクセスが許可されるターゲットサービスを選択できます。デフォルト設定は、*HTTP*(ポート80)、*HTTPS*(ポート443)、*FTP*(ポート21)、*LDAP*(ポート389)、*LDAP-SSL*(ポート636)、*Web フィルタ*(ポート8080)、*UTMSpam Release*(ポート3840~ 4840)、および *UTMWebAdmin*(ポート4444)などのターゲットサービス(ポート)で構成されています。これらは、通常は安全に接続でき、ブラウザで一般に使用されています。

デフォルトの文字コード: このオプションは、*ダウンロードマネージャ*ウィンドウでプロキシがファイル名をどのように表示するかに影響を与えます。外国語の文字セットでエンコードされているURL(およびURLで参照されるファイル名)は、サーバが別の文字セットを送信する場合を除き、ここで指定されている文字セットからUTF-8に変換されます。ダブルバイト文字セットを使用する国または地域では、このオプションを当該国または地域の「ネイティブ」文字セットに設定する必要があります。

検索ドメイン: ここで、最初のDNSルックアップで結果が返されなかった("NXDOMAIN")場合に検索される追加のドメインを追加することができます。最初のDNSルックアップの次に、2番目のDNS

要求が開始され、ここで指定したドメインをオリジナルのホスト名に追加します。例：ユーザがアドレスwiki.intranet.example.comとして`http://wiki`と入力し*ます*。ただし、URLは、ドメイン検索フィールドに*intranet.example.com*と入力していなければ解決できません。

認証タイムアウト: この設定で、ブラウザ認証モードでログイン後にユーザがブラウズ可能な時間の長さ（秒単位）を設定することができます。ユーザがログアウトタブを開いている場合、タブを閉じ、さらに認証タイムアウトまで、ユーザは再認証せずにブラウズを継続することができます。

またこの設定で、*オーバーライドのブロック*または*警告手順*が継続する時間の長さ（秒単位）を設定することができます。

認証レルム: 認証レルムとは、プロキシが*基本ユーザ認証*モードで機能しているときに、ブラウザが認証要求とともに表示する送信元の名前です。認証レルムは、RFC 2617に基づいて保護スペースを定義します。ここでは任意の文字列を指定できます。

透過モードスキップリスト

このオプションは、Webフィルタを透過モードで実行している場合のみ有用です。*透過モード時にスキップするホスト/ネット*ボックスにリストされているホストとネットワークは、HTTPトラフィックの透過的インターセプションの対象とはなりません。ボックスは、送信元ホスト/ネットワーク用に1つ、宛先ホスト/ネットワーク用に1つあります。これらのホストとネットワークに対して、HTTPトラフィックを（プロキシなしで）許可するには、*リスト内のホスト/ネットワークのHTTPトラフィックを許可*チェックボックスにチェックを入れます。このチェックボックスにチェックを入れない場合は、ここでリストされているホストとネットワークに特定のファイアウォールルールを定義する必要があります。

プロキシ自動設定

プロキシの自動設定とは、ブラウザにフェッチされるプロキシ自動設定ファイル（PACファイル）を一元的に提供するための機能です。ブラウザはこれを受けて、PACファイルに記述された詳細に従ってプロキシ設定を構成します。

PAC ファイルの名前は *wpad.dat*、MIME タイプは `application/x-ns-proxy-autoconfig` で、UTM から提供されるものです。このファイルには、たとえば次のように、テキストボックスに入力した情報が含まれています。

```
function FindProxyForURL(url, host)
{ return "PROXY proxy.example.com:8080; DIRECT"; }
```

上の関数は、すべてのページ要求をポート`8080`上の`proxy.example.com`というサーバのプロキシにリダイレクトするようブラウザに指示しています。プロキシに到達できなければ、インターネットへの直接接続が確立されます。

ホスト名は、`${asg_hostname}`という変数としても指定できます。これは、Sophos UTM Managerを使用して、同じPACファイルを複数のSophos UTMアプライアンスにインストールする場合などに便利です。変数には、該当するUTMのホスト名が挿入されます。上記の例にある変数を使用すると、次のようになります。

```
function FindProxyForURL(url, host)
{ return "PROXY ${asg_hostname}:8080; DIRECT"; }
```

ネットワークでPACファイルを提供するには、次の方法があります。

- ブラウザ設定経由で提供する:*プロキシ自動設定の有効化*オプションを選択すると、UTM Webフィルタ経由でPACファイルを使用できるようになります。このとき、次のようなURLを使用します。`http://IP-of-UTM:8080/wpad.dat`。このファイルを使用するには、プロキシを使用するブラウザの自動プロキシ構成設定にこのURLを入力します。

- DHCP経由で提供する:DHCPサーバがクライアントのIPアドレスと併せてPACファイルのURLを受け渡すようにすることもできます。これには、DHCPサーバの設定で*HTTPプロキシ自動設定の有効化*オプションを選択します(*ネットワークサービス* > *DHCP*の章を参照してください)。これにより、ブラウザがPACファイルを自動的に取得し、それに従って設定を構成します。

> 注 – DHCP経由での提供は、マイクロソフトのInternet Exploreのみで機能します。その他すべてのブラウザでは、PACファイルを手動で提供する必要があります。

URL分類親プロキシ

直接インターネットアクセスがない場合、URL分類ルックアップにプロキシサーバを入力します。このオプションは、エンドポイントプロテクションが有効になっている場合、またはローカルルックアップを行っている場合のみ使用可能です。ローカルルックアップでは、このオプションはUTMへの分類更新のダウンロードに使用されるプロキシを設定します。

Webキャッシング

キャッシングの有効化:このオプションが有効になっている場合、Webフィルタはオンディスクオブジェクトキャッシュを保持して、アクセス頻度が高いWebページへの要求を高速化します。

- **SSL**コンテンツのキャッシュ:このオプションを有効にすると、SSL暗号化されたデータは、暗号化されていない状態でディスクに保存されます。

- **Cookie**を含むコンテンツをキャッシュ:Cookieは、一般に認証目的で使用されます。このオプションを有効にすると、Cookieが含まれるHTTP応答もキャッシュされます。複数のユーザが同じページを要求している場合、あるユーザのCookieが含まれるキャッシュページが他の

ユーザに提供される可能性があるため、この設定は重大です。

重要 – SSLまたはCookieコンテンツ(あるいはその両方)をキャッシュすると、SuperAdmin権限を持つすべてのユーザがコンテンツを閲覧できるため、セキュリティ上の重要な問題です。

- **Sophosエンドポイント用アップデートの強制キャッシュ**: 有効にすると、エンドポイントからのSophos自動アップデート(SAU)要求に関連する特定のデータがキャッシュされます。エンドポイントプロテクションを使用する場合、機能を有効にすることを推奨いたします。無効にすると、このタイプのデータはキャッシュされません。これは、多数のエンドポイントがインターネットにある更新サーバから同時にデータをダウンロードしようとする際のアップリンク飽和につながります。

キャッシュをクリア: *キャッシュをクリア*をクリックすると、キャッシュされたすべてのページを削除できます。

ストリーミング設定

ストリーミングコンテンツに対するコンテンツスキャンのバイパス: このオプションを選択すると、一般的な音声・動画ストリーミングコンテンツがコンテンツスキャンの対象外となります。このオプションを無効にすると、大部分のメディアストリームは事実上無効になります。これは、このようなストリームを合理的な時間内でスキャンすることができないためです。そのため、このオプションは選択することを推奨します。

Apple OpenDirectoryのシングルサインオン

認証方式として*Apple OpenDirectory SSO*を使用している場合、認証が適切に機能するためには、MAC OS Xシングルサインオン Kerberos鍵ファイルをアップロードする必要があります。この鍵ファイルを生成し、フォルダアイコンをクリックしてアップロードします。鍵ファイルの生成方法について詳しくは、Kerberosのマニュアルを参照してください。

エンドユーザページの証明書

UTMは、ユーザ通知の提供、ブラウザ認証の実行、その他のユーザインタラクションの安全性確保のためにHTTPSを使用します。デフォルトでは、UTMはこれらのHTTPS接続に対し、自動的生成証明書を使用します。このオプションにより、エンドユーザに表示されるHTTPSページ用にカスタム証明書を使用することができます。これらのHTTPS接続に対し、独自のカスタム証明書を使用するには、まず初めに*リモートアクセス* > *証明書管理* > *証明書*でカスタム証明書をアップロードし、次に選択し、ここで設定を更新します。

注 – 指定の*ホスト名*は使用している証明書に対するベースドメインとなります。次に、UTMは*パススルー*をプリペンドします。または、そのドメインに対して*パススルー6.*をプリペンドします。ドメインにおける任意のホストにプリペンドするため、証明書は、一般名、サブジェクトの別名、またはとして最も一般的なワイルドカード証明書として*パススルー*(*およびパススルー6*)に対し有効である必要があります。さらに、特定のIPアドレスに対し*パススルー*および*パススルー6*のDNSを設定しなければなりません。UTMをDNSサーバとして使用する場合、これは自動的に行われます。代替DNSサーバを使用している場合、そこでこれらのエントリを作成する必要があります。

9.4 ポリシヘルプデスク

*Webプロテクション > ポリシヘルプデスク*ページで、既存のポリシに対してURLをテストし、ユーザの割当てステータス評価またはリセットできます。*ポリシテスト*タブを使用してURLをテストでき、*割当てステータス*タブを使用してユーザの現在の割当てステータスを見ることができます。

9.4.1 ポリシテスト

*Webプロテクション > ポリシヘルプデスク > ポリシテスト*ページを使用して、既存のWebフィルタプロファイルに対してURLをテストすることができます。現在のポリシに対してURLをテストするには、次の手順に従います。

1. テストしたい**URL**を入力します。
2. **送信元IPアドレスを設定します。**
   送信元ネットワークが異なると、Webフィルタプロファイルも異なります。ネットワークが複数のプロファイルに含まれている場合、優先順位の最も高いプロファイルがポリシテスト使用されます。
3. **オプションで、テストを要求しているユーザを入力します。**
   ユーザは、異なるWebフィルタプロファイルに属することがあります。
4. **オプションで、要求の時刻を入力します。**
   Webフィルタプロファイルは、指定時刻に基づくルールを持つように設定できます。
5. *テスト*をクリックします。

テストパラメータの結果が、*ポリシテスト結果*ボックスに表示されます。

注 – Webフィルタプロファイルに対してURLをテストする場合、*Webプロテクション > ポリシテスト*ページはコンテンツをダウンロードしたり、マルウェア、MIMEタイプ、ファイル拡張子をチェックしたりすることはありません。実際のフィルタリングの動作は、そのURLがホストしているコンテンツによって異なります。

注 – テストが適切に機能するには、*定義とユーザ > 認証サービス > サーバ*ページで正しい認証サーバを追加する必要があります。

9.4.2 割当てステータス

*Webプロテクション > ポリシヘルプデスク > 割当てステータス*ページを利用して、ユーザに残っている割当て分数をレビューできます。また、時間切れのユーザの割当てをリセットできます。

ユーザまたは一連のユーザの割当てをレビューするには:

1. ***割当てステータス*タブで、レビューするユーザを特定します。**
   ある程度割当て時間を使っているユーザがリストされます。検索テキストボックスを使用して、特定のユーザを検索します。または、フィルタアクションを行って結果を絞り込みます。特定のユーザの割当ての残り時間が示されます。

2. **ユーザを選択して、割当て時間をリセットします。**
   リセットするユーザの横のチェックボックスを選択します。または、最上部のチェックボックスをクリックして、現在表示されているすべてのユーザを選択します。

3. ***リセット*をクリックします。**
   選択したユーザの割当て時間がリセットされ、フルの割当て時間が与えられます。通常、全ユーザの割当て時間は午前0時にリセットされます。

9.5 アプリケーション コントロール

UTMのアプリケーション制御機能を使用すると、トラフィックの種類に基づいてネットワークトラフィックをシェーピングおよびブロックすることができます。UTMのWebフィルタリング機能（Webフィルタリングの章を参照）と違い、アプリケーション制御分類エンジンを使用すると、ネットワークトラフィックを、プロトコルや URL 単位ではなく、よりきめ細かい基準で識別することができます。これは、Webトラフィックに関して特に便利です。Webサイトへのトラフィックは、通常ポート80 でHTTPプロトコルを使用するか、ポート443 でHTTPSプロトコルを使用しています。特定のWebサイト（facebook.comなど）へのトラフィックをブロックしたい場合、WebサイトのURL（Webフィルタリング）に

基づいてブロックすることができます。あるいは、ネットワークトラフィック分類を利用して、あらゆるURLから独立してfacebookトラフィックをブロックすることができます。

UTMの分類エンジンは、ネットワークトラフィックの分類にレイヤ7パケット検査を使用します。

アプリケーションコントロールは2つの方法で使用できます。最初のステップでは、*ネットワーク可視化*ページでアプリケーション制御全般を有効にする必要があります。これにより、アプリケーションが一定の範囲で「可視化」されます。これをこのまま（または、特定の時間だけ）残し、ユーザに使用されているアプリケーション（フローモニタ、ロギング、レポーティングなど）を確認することができます。2番目のステップでは、特定のアプリケーションをブロックし、他のアプリケーションは許可することができます。これには、*アプリケーション制御ルール*ページで作成するルールを使用します。さらに、トラフィックシェーピングを使用して、定義したアプリケーションのトラフィックに特権を与えることができます。この設定は、SophosのQoS機能で行います。

9.5.1 ネットワーク可視化

*Webプロテクション > アプリケーション制御 > ネットワーク可視化*ページでは、アプリケーション制御を有効または無効にすることができます。

アプリケーションコントロールを有効化すると、すべてのネットワークトラフィックが、その分類に応じて分類またはロギングされます。現在のネットワークトラフィックは、フローモニタに、タイプに関する詳細な情報と共に表示されます（*フローモニタ*の章を参照）。たとえば、HTTPトラフィックに関する情報は、もとのアプリケーション（「twitter」、「facebook」など）までドリルダウンされます。フローモニタを開くには、*フローモニタ*セクションで目的のインタフェースを選択し、*フローモニタを開く*ボタンをクリックします。

ログとレポートでは、ネットワークトラフィックとその分類に関する幅広い情報と、これらのアプリケーションを使用するクライアントとサーバの情報が表示されます。ログとレポートについて詳しくは、*ログとレポート*の章で、*ログファイルの閲覧*セクションを参照するか（ログ）、*ネットワーク使用率 > 帯域使用状況*セクションおよび*Webプロテクション > アプリケーション制御*セクションを参照してください（レポート）。

9.5.2 アプリケーション コントロール ルール

*Webプロテクション > アプリケーション制御 > アプリケーション制御ルール*ページでは、ネットワークに対してトラフィックをブロックするか、または明示的に許可するアプリケーションを定義するネットワークトラフィック分類に基づいて、ルールを作成することができます。

デフォルトでは、アプリケーションコントロールを有効にするとすべてのネットワークトラフィックが許可されます。

アプリケーションコントロールルールの作成は、このページでもフローモニタでも可能です。フローモニタの方が使いやすいですが、ルールを作成できるのは、ネットワークで現在モニタリングされているトラフィックに対してのみです。

アプリケーションコントロールルールを作成するには、以下の手順に従います。

1. *アプリケーションコントロールルール***タブで、***新規ルール***をクリックします。**
   *ルールの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前（オプション）: ルールの名前を入力します。フィールドを空のままにすると、システムがルールの名前を生成します。

   グループ: *グループ*オプションを使用すると、ルールを論理的にグループ化できます。リストの上部にあるドロップダウンリストを使用すると、ルールをグループ別にフィルタできます。グループ化は表示用のみで、ルールの一致には関係ありません。新しいグループを作成するには、<<*新規グループ*>>エントリを選択し、グループを説明する名前を*名前*に入力します。

   優先順位: ルールの優先順位を定義する位置番号。番号が小さいほど優先順位が高くなります。ルールは昇順に照合されます。あるルールが一致すると、それ以降、それより大きい番号のルールは評価されません。

   アクション: トラフィックをブロックするか許可するかを選択します。

   制御基準: アプリケーションタイプに基づいてトラフィック制御するか、分類に基づくダイナミックフィルタによって制御するかを選択します。

   - *アプリケーション*: トラフィックは、アプリケーションに基づいてコントロールされます。*制御するアプリケーション*ボックスでアプリケーションを1つ以上選択します。
   - *ダイナミックフィルタ*: トラフィックは、カテゴリに基づいて制御されます。*制御するカテゴリ*ボックスで分類を1つ以上選択します。

   制御する*アプリケーション/カテゴリ*: フォルダアイコンをクリックして、アプリケーション/カテゴリを選択します。ダイアログウィンドウが開きます。これについては、次のセクションで詳しく説明します。

   注 – 一部のアプリケーションはブロックすることができません。これは、Sophos UTMの適切なオペレーションのために必要です。このようなアプリケーションは、*アプリケーション選択*ダイアログウィンドウのアプリケーションテーブルでチェックボックスがオフになっています。たとえば、*WebAdmin*、*Teredo*、*SixXs*（IPv6トラフィック用）、*Portal*（ユーザーポータル

のトラフィック用）などが該当します。ダイナミックフィルタを使用すると、これらのアプリケーションのブロックも自動的に制限されます。

生産性（*ダイナミックフィルタ*のみ）：選択した生産性スコアが反映されます。

リスク（*ダイナミックフィルタ*のみ）：選択したリスクスコアが反映されます。

対象ネットワーク：このルールによってネットワークトラフィックをコントロールするネットワークまたはホストを選択するか、このボックスに追加します。これは、送信元ホスト/ネットワークだけに適用されます。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

ログ：このオプションはデフォルトでオンになっており、ルールと一致するトラフィックのロギングが有効になります。

コメント（オプション）：説明などの情報を追加します。

3. ***保存*をクリックします。**
新しいルールが*アプリケーション制御ルール*リストに表示されます。

アプリケーションまたはカテゴリの選択ダイアログウィンドウ

アプリケーションコントロールルールを作成する際は、*管理するアプリケーション(カテゴリ)を1つ以上選択してください*というダイアログウィンドウからアプリケーションまたはアプリケーションカテゴリを選択する必要があります。

ダイアログウィンドウの下部に表示されるテーブルには、選択可能なアプリケーションまたは定義したカテゴリに属するアプリケーションが表示されます。デフォルトでは、すべてのアプリケーションが表示されます。

ダイアログウィンドウの上部には、テーブルに表示されるアプリケーション数を制限するための3つの設定オプションがあります。

- *カテゴリ*：アプリケーションはカテゴリ別にグループ分けされています。このリストには、利用可能なすべてのカテゴリが表示されます。デフォルトでは、すべてのカテゴリが選択されています。つまり、下部に表示されるテーブルには、利用可能なすべてのアプリケーションが表示されます。表示されるアプリケーションを特定のカテゴリに絞り込むには、クリックしてカテゴリリストを開き、1つ以上のカテゴリを選択します。
- 生産性：アプリケーションは、生産性への影響（つまり生産性にこのアプリケーションが与える影響の度合い）によっても分類されています。例：一般的なビジネスソフトウェアのSalesforceのスコアは5です。つまり、これを使用することで生産性が向上します。一方、オン

ラインゲームのFarmvilleのスコアは1で、これを使用すると生産性が低下します。ネットワークサービスDNSのスコアは3で、生産性への影響は中立的です。

- リスク: アプリケーションは、使用時のリスク(マルウェア、ウイルス感染、攻撃)によっても分類されています。数値が高いほど、リスクも高くなります。

ヒント – それぞれのアプリケーションには情報アイコンがあり、クリックすると各アプリケーションの説明が表示されます。テーブルヘッダのフィルタフィールドを使用して、テーブル内を検索することができます。

次に、*新規ルール作成*ダイアログウィンドウで選択したコントロールのタイプに応じて、以下を行います。

- ダイナミックフィルタでコントロールする場合 : *カテゴリ*ボックスでカテゴリを選択し、*適用*をクリックして、選択したカテゴリをルールに適用します。
- アプリケーションでコントロールする場合 : テーブルで、アプリケーションの前のチェックボックスをクリックし、コントロール対象のアプリケーションを選択します。*適用*をクリックして、選択したアプリケーションをルールに適用します。

*適用*をクリックするとダイアログウィンドウが閉じ、アプリケーションルールの設定の編集を続けることができます。

9.5.3 詳細

*Webプロテクション > アプリケーション制御 > 詳細*ページでは、アプリケーション制御の詳細オプションを設定できます。

アプリケーション制御スキップリスト

このボックスにリストされているホストとネットワークは、アプリケーションコントロールの監視対象とはならないため、アプリケーションコントロールで管理することも、サービス品質のアプリケーションセレクタで管理することもできません。これは、送信元および宛先ホスト/ネットワークの両方に適用されます。

9.6 FTP

*Webプロテクション > FTP*タブでは、FTPプロキシを設定できます。FTP(*ファイル転送プロトコル*)とは、インターネット上でファイルを交換するために広く使用されているプロトコルです。Sophos UTMは、ネットワークを通過するすべてのFTPトラフィックの仲介役となるプロキシサービスを提供しま

す。FTP プロキシには、FTP トラフィックのウイルススキャンや、FTP プロトコル経由で転送される特定のファイルタイプのブロックといった便利な機能が用意されています。

FTPプロキシには、FTPトラフィックのウイルススキャンや、FTPプロトコル経由で転送される特定のファイルタイプのブロックといった便利な機能が用意されています。続いて、クライアントから見えない状態でプロキシが要求に代わって新しいネットワーク接続を開始します。このモードのメリットは、その他の管理やクライアント側の設定が必要ないということです。

9.6.1 グローバル

*Webプロテクション > FTP > グローバル*タブでは、FTPプロキシの基本設定を構成できます。

FTPプロキシを設定するには、次の手順に従ってください。

1. ***グローバル*タブで、FTPプロキシを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、*FTP設定*エリアが編集可能になります。

2. **許可するネットワークを選択します。**
   FTPプロキシの使用を許可するネットワークを選択します。

3. **オペレーションモードを選択します。**
   FTPプロキシのオペレーションモードを選択します。次のモードを使用できます。

   - 透過：プロキシは、クライアントの要求をターゲットサーバに転送し、コンテンツをスキャンします。クライアント側での設定は不要です。
   - 非透過：このモードを使用する場合、FTPクライアントを設定する必要があります。ゲートウェイのIPアドレスとポート`2121`を使用します。
   - 両方：このモードを使用すると、一部のクライアントには透過モードを、他のクライアントには非透過モードを使用することができます。非透過モードで機能させるFTPクライアントを、ゲートウェイのIPアドレスとポート`2121`でプロキシを使用するように設定します。

4. ***適用*をクリックします。**
   設定が保存されます。

   トグルスイッチが緑色に変わります。

注 – FTPプロキシは、Active Directory認証を使用するFTPサーバとは通信できません。FTPクライアントがこのようなFTPサーバに接続できるようにするには、このサーバをFTPプロキシのスキップリストに追加します。スキップリストの設定は、*詳細*タブで行います。

9.6.2 ウイルス対策

Webプロテクション > *FTP* > *ウイルス対策*タブには、ウイルス、ワーム、その他のマルウェアなどの有害で危険なコンテンツを伝送するFTPトラフィックに対して講じることができるあらゆる対策が含まれています。

ウイルス対策スキャンを使用：このオプションを選択すると、FTPトラフィックがスキャンされます。Sophos UTMは、最高のセキュリティを実現するさまざまなウイルス対策エンジンを備えています。

- シングルスキャン： デフォルト設定。*システム設定* > *スキャン設定*タブに定義されたエンジンを使用して最高レベルのパフォーマンスを実現します。
- デュアルスキャン：各トラフィックに対し、異なるウイルススキャナを使用してスキャンを2回行うことにより、検知率を最大限に高めます。デュアルスキャンは、ベーシックガードサブスクリプションでは使用できません。

最大スキャンサイズ：ウイルス対策エンジンでスキャンする最大ファイルサイズを指定します。このサイズを超えるファイルはスキャン対象外となります。

設定を保存するには*適用*をクリックします。

注 – アーカイブ内のファイル（例、zipファイル）は、ブロックするファイルタイプ、ブロックする拡張子、ブロックするMIMEタイプではスキャンされません。こうしたアーカイブ内のファイルからネットワークを保護するには、zip、rar、などのアーカイブファイルタイプのブロックを検討してください。

ファイル拡張子フィルタ

この機能では、ファイルの拡張子（実行可能バイナリなど）に基づいて、*ブロック対象ファイル拡張子*ボックスにファイル拡張子がリストされているタイプのファイルを伝送するFTP転送をWebトラフィックからフィルタします。ファイル拡張子を追加したり、ブロック対象から外すファイル拡張子を削除したりすることができます。ファイル拡張子を追加するには、*ブロックするファイル拡張子*ボックスの「+」アイコンをクリックし、ブロックする拡張子（exeなど）を入力します（区切り記号のドットは不要です。）。設定を保存するには*適用*をクリックします。

9.6.3 除外

FTP > *除外*タブでは、FTPプロキシの提供する選択可能なセキュリティオプションから除外するホワイトリストのホスト/ネットワークを定義することができます。

除外ルールを作成するには、次の手順に従います。

1. ***除外*タブで、*新規除外リスト*をクリックします。**
   *除外リストを追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:この除外ルールを説明する名前を入力してください。

   実行しないチェック:スキップするセキュリティチェックを選択します。

   - ウイルス対策チェック:選択すると、ウイルスやトロイの木馬などの好ましくないコンテンツがトラフィックに含まれていないかチェックするウイルススキャンが無効になります。
   - 拡張子ブロック:選択すると、ファイル拡張子フィルタが無効になります。このフィルタは、ファイル拡張子に基づいてファイル転送をブロックするために使用します。
   - 許可サーバ:選択すると、*詳細*タブで設定できる、許可サーバのチェックが無効になります。選択すると、選択したクライアントのホスト/ネットワークはすべてのFTP サーバにアクセスできるようになり、選択したサーバのホスト/ネットワークはすべてのクライアントが許可されます。

   クライアントホスト/ネットワークで除外:このオプションを選択すると、*クライアントホスト/ネットワーク*ボックスが開きます。この除外ルールのセキュリティチェックから除外するクライアントホスト/ネットワークを選択します。

   サーバホスト/ネットワークで除外:このオプションを選択すると、*サーバホスト/ネットワーク*ボックスが開きます。この除外ルールのセキュリティチェックから除外するサーバホスト/ネットワークを選択します。

   コメント(オプション):説明などの情報を追加します。

3. ***保存*をクリックします。**
   新しい除外ルールが*除外*リストに表示されます。

除外ルールを編集または削除するには、対応するボタンをクリックします。

9.6.4 詳細

*FTP > 詳細*タブでは、FTPプロキシの透過モードをスキップできるホストとネットワークを指定できます。さらに、アクセスを許可するFTP サーバを定義できます。

FTPプロキシスキップリスト

ここにリストされるホストおよびネットワーク(FTP クライアントならびにFTP サーバ)は、FTPトラフィックの透過的インターセプションの対象から除外されます。ただし、これらのホストおよびネット

ワークでFTPトラフィックを許可するには、*リスト内のホスト/ネットワークのFTPトラフィックを許可*チェックボックスにチェックを入れます。このチェックボックスにチェックを入れない場合は、ここでリストされているホストとネットワークに特定のファイアウォールルールを定義する必要があります。

注 – FTPプロキシは、Active Directory認証を使用するFTPサーバとは通信できません。FTPクライアントがこのようなFTPサーバに接続できるようにするには、このサーバをFTPプロキシのスキップリストに追加します。

FTPサーバ

ホスト/ネットワークからのアクセスを許可するFTPサーバまたはネットワークを選択または追加します。一部のFTP クライアントやFTP サーバがこのリストをバイパスするように、*除外*タブで除外を作成できます。

10 Eメールプロテクション

この章では、Sophos UTMの基本的なEメールプロテクション機能を設定する方法を説明します。WebAdmin の*Eメールプロテクション統計*ページには、メール送信者、メール受信者、スパム送信元(国別)、検知数によるマルウェアのその日の上位 10件までに加え、同時接続の概要が表示されます。各セクションには*詳細*リンクがあります。リンクをクリックするとWebAdminのそれぞれのレポーティングセクションが表示され、そこでさらなる統計情報を参照できます。

この章には次のトピックが含まれます。

- SMTP
- SMTPプロファイル
- POP3
- 暗号化
- SPX暗号化
- 隔離レポート
- メールマネージャ

10.1 SMTP

*Eメールプロテクション > SMTP*メニューでSMTPプロキシを設定できます。SMTP は*簡易メール転送プロトコル* の略で、メールをメールサーバーに転送するために使用されるプロトコルです。Sophos UTMはSMTPのためのアプリケーションレベルのゲートウェイを装備しており、これを使用して内部メールサーバをリモートの攻撃から守り、さらに強力なウイルススキャンおよびメールフィルタサービスを提供できます。

注 – SMTP プロキシを正しく使用するには、有効なネームサーバー(DNS)を設定する必要があります。

10.1.1 グローバル

*Eメールプロテクション > SMTP > グローバル*タブで、SMTP *設定に対して*シンプルモード*を使用するか*プロファイルモードを使用するかを決定できます。

1. **SMTPを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチが緑色になり、*設定モード*エリアが編集可能になります。

2. **設定モードを選択します。**
   シンプルモード: すべてのドメインが同じ設定を共有している場合はこのモードを使用します。ただし、ドメイン名、メールアドレス、およびホストに基づいて除外ルールを定義することもできます。これは*プロファイルモード*と異なり機能的な制限はありません。

   プロファイルモード: (ベーシックガードサブスクリプションでは使用できません。)このモードでは、個々のドメインあるいはドメイングループのアンチスパムやウイルス対策などのグローバル設定を、*SMTPプロファイル*メニューでそれらのプロファイルを作成することで、上書きまたは拡張できます。*SMTP*メニューで行った設定は、依然として指定のドメインに適用され、プロファイルのデフォルトとなります。*プロファイルモード*には、UTMのプロファイルモードや動作の推奨設定について、いくつかの注意事項があります。

3. ***適用*をクリックします。**
   選択したモードが有効になります。

SPXグローバルテンプレート

SPX暗号化が有効な場合、このセクションを利用することができます。ドロップダウンリストから、グローバルに使用されるSPXテンプレートを選択します。SMTPをシンプルモードで使用している場合、このテンプレートはすべてのSMTPユーザに使用されます。SMTPをプロファイルモードで使用している場合、このテンプレートは個別に選択されていないSPXテンプレートのすべてのSMTPプロファイルに使用されます。

ライブログ

*SMTPライブログ*は、SMTPプロキシのアクティビティをログし、すべての受信メールを表示します。ボタンをクリックして、新しいウィンドウでライブログを開きます。

10.1.2 ルーティング

*ルーティング*タブで、SMTPプロキシのドメインとルーティングターゲットを設定し、受信者の検証方法を定義します。

SMTPプロキシのルーティングを設定するには、以下の手順に従います。

1. **内部ドメインを入力します。**
   メールのドメインを入力するには、*ドメイン*ボックスの「+」アイコンをクリックします。

表示されたテキストボックスに、example.comの形式でドメインを入力し、*適用*をクリックします。すべてのドメインがリストされるまでこのステップを繰り返します。また、ワイルドカードを異なる方法で使用可能です。例：*.me.mycompany.de、*.mycompany.de、*.me*.mycompany.*e、**.mycompany.*。「*」のみを使用することはできません。

プロファイルモード:グローバル設定を使用するドメインのみを入力します。他のすべてのドメインは、それぞれのプロファイルにリストします。

2. **内部サーバを指定します。**
*ルーティング方式*ドロップダウンリストで、上記でリストしたドメイン宛てのメールの転送先ホストを選択します。一般的なターゲットホストとしては、ローカルネットワーク上のMicrosoft Exchange Serverが挙げられます。さまざまなサーバタイプから選択できます。

   - スタティックホストリスト: *ホストリスト*ボックスで、ターゲットルートのホスト定義を選択します。基本的なフェイルオーバー用に複数のホスト定義を選択できます。最初のホストへの配信に失敗すると、メールは次のホストにルーティングされます。ただし、ホストのスタティック（静的）な順序は、現在のバージョンのSophos UTMでは決定できず、やや偶発的に決定されます。基本的な負荷分散機能をさらに効率よく達成できるようにホストグループへの配信をランダム化するには、*DNS ホスト名* ルートタイプを使用し、複数の A レコードを持つホスト名を指定します（*A レコード*または*アドレスレコード*は、ホスト名をIP アドレスにマップします）。
   - **DNS**ホスト名：ターゲットルートの*完全修飾ドメイン名*（FQDN）を指定します（例：exchange.example.com）。複数のAレコードを持つDNS名を選択すると、各サーバへのメールはランダムに配信されます。さらに、1台のサーバに障害が発生すると、そのサーバ宛てのすべてのメールは残りのサーバに自動的にルーティングされます。
   - **MX**レコード: MXレコードを使用して、お使いのドメインにメールをルーティングすることもできます。このルートタイプを選択すると、Sophos UTMのメール転送エージェントは、受信者のドメイン名（メールアドレスの「@」文字に続く部分）のMXレコードを要求するDNSクエリを行います。ゲートウェイが上記で指定したドメインのプライマリMXではないことを確認する必要があります。なぜなら、自らにはメールを配信しないからです。

3. ***適用*をクリックします。**
設定が保存されます。

受信者検証

受信者検証：ここでメール受信者を確認するかどうかと確認方法を指定できます。

- コールアウト使用：受信者検証の要求がサーバに送信されます。
- **Active Directory**：受信者検証の要求がActive Directoryサーバに送信されます。Active Directoryを使用するには、*定義とユーザ* > *認証サービス* > *サーバ*で指定されたActive Directoryサーバを備えていることが必要です。ベースDNを*代替ベースDN*フィールドに入力します。

> 注 – Active Directory 受信者検証を使用すると、サーバーが応答しない場合にメッセージがバウンスされる場合があります。

- オフ：受信者確認は完全にオフにできますが、推奨されません。なぜなら、オフにすると、スパムトラフィックが増大して、辞書攻撃の危険性が高まるからです。この結果、隔離場所が迷惑メールで溢れてしまうことになります。

設定を保存するには*適用*をクリックします。

10.1.3 ウイルス対策

*ウイルス対策*タブには、ウイルス、ワーム、その他のマルウェアなどの有害で危険なコンテンツを含むメールに対するさまざまな対策が含まれています。

> 注 – 送信メールは、*リレー*タブの*リレー(送信)メッセージのスキャン*が選択されている場合にスキャンされます。

SMTPトランザクション中のスキャン

*SMTPトランザクション時にマルウェアをリジェクト*チェックボックスにチェックを入れることで、SMTPトランザクション中にスキャンを行い、マルウェアが含まれている場合は拒否（リジェクト）することができます。

プロファイルモード：この設定はプロファイルごとには変更できません。1人以上の受信者がいるメッセージで、受信者の1人のプロファイルで*ウイルス対策スキャン*がオフになっている場合は、この機能はスキップされます。したがって、以下の通常のウイルス対策設定を*ブラックホール*あるいは*隔離*のいずれかの設定にしておくことをお勧めします。

設定を保存するには*適用*をクリックします。

ウイルス対策スキャン

このオプションでは、ウイルス、トロイの木馬、疑わしいファイルタイプなどの不要なコンテンツがないかどうか、メールをスキャンします。悪意のあるコンテンツを含むメッセージはブロックされて、

メールの隔離場所に保存されます。ユーザは、Sophos ユーザポータルまたはデイリーの隔離レポートで、隔離されたメッセージを確認してリリースできます。ただし、悪意のあるコンテンツを含むメッセージは、メールマネージャで管理者のみが隔離からリリースできます。

ウイルス対策: 悪意あるコンテンツを含むメッセージの処理方法を設定できます。次の作業を実行できます。

- *オフ*: ウイルス対策スキャンを実行しません。
- *ブラックホール*: メッセージは受信後、ただちに削除されます。送信メッセージは、意図しないメールの紛失を回避するために、ブラックホール化されることがありません。代わりに、隔離されます。
- *隔離*: メッセージはブロックされ、メールの隔離場所に保存されます。隔離されたメッセージは、ユーザポータルまたはデイリーの隔離レポートで確認できます。悪意のあるコンテンツを含むメッセージを隔離場所からリリースできるのは、管理者だけです。

Sophos UTMは、最高のセキュリティを実現するさまざまなウイルス対策エンジンを備えています。

- *シングルスキャン*: デフォルト設定。*システム設定* > *スキャン設定*タブに定義されたエンジンを使用して最高レベルのパフォーマンスを実現します。
- *デュアルスキャン*: 各トラフィックに対し、異なるウイルススキャナを使用してスキャンを2回行うことにより、検知率を最大限に高めます。デュアルスキャンは、ベーシックガードサブスクリプションでは使用できません。

スキャンできないコンテンツ、暗号化されたコンテンツの隔離: このオプションを選択して、コンテンツをスキャンできなかったメールを隔離します。スキャンできないコンテンツは、暗号化されたもの、破損したアーカイブ、またはサイズが大きすぎるコンテンツの他、スキャナの不具合などの技術的な問題による場合があります。

設定を保存するには*適用*をクリックします。

MIMEタイプフィルタ

MIMEタイプのフィルタはMIMEタイプのEメールコンテンツを読みます。さまざまなMIMEタイプをどう取り扱うかを定義できます。

- *オーディオコンテンツを隔離*: このチェックボックスにチェックを入れると、mp3あるいはwavファイルなどの音声コンテンツが隔離されます。
- *ビデオコンテンツを隔離*: このチェックボックスにチェックを入れると、mpgあるいはmovファイルなどの動画コンテンツが隔離されます。
- *実行形式コンテンツを隔離*: このチェックボックスにチェックを入れると、exeファイルなどの実行形式コンテンツが隔離されます。

隔離する他のタイプ: 上記以外のMIMEタイプを隔離するには、*隔離する他のタイプ*ボックスの「+」アイコンをクリックし、MIMEタイプ(例:`image/gif`)を入力します。スラッシュ右側にワイルドカード(`*`)を使用できます(例:`application/*`)。

ホワイトリスト化するタイプ: このボックスを使用して一般的に信頼できるMIMEタイプを許可します。MIMEタイプを追加するには*ホワイトリストのコンテンツタイプ*ボックスの「+」アイコンをクリックし、MIMEタイプを入力します。設定を保存するには*適用*をクリックします。

MIMEタイプ	**MIMEタイプのクラス**
audio/*	音声ファイル
video/*	動画ファイル
application/x-dosexec	アプリケーション
application/x-msdownload	
application/exe	
application/x-exe	
application/dos-exe	
vms/exe	
application/x-winexe	
application/msdos-windows	
application/x-msdos-program	

表2: MIMEタイプフィルタで認識されるMIMEタイプ

ファイル拡張子フィルタ

この機能は、ファイル拡張子に基づいて特定タイプのファイル(実行可能ファイルなど)を含むメールを(警告付きで)フィルタリングし、隔離します。ファイル拡張子を追加するには、*ブロック対象ファイル拡張子*ボックスの「+」アイコンをクリックし、制限するファイル拡張子(例:`exe`、`jar`(区切り文字のドットなし))を入力します。設定を保存するには*適用*をクリックします。

ウイルス対策チェックフッタ

各送信メールで、悪意あるコンテンツについてメールをスキャン済みであることをユーザに知らせる特別なフッタを追加してカスタマイズできます。ただし、*リレー*タブの*リレー送信メッセージのスキャン*チェックボックスが選択されている場合にのみフッタが追加されます。さらに、ウイルス対策チェックフッタは、メールが返信の場合追加されません。(つまり、*In-Reply-To*ヘッダを持つもの)

またはメールのコンテンツタイプを判定できない場合は、メールに追加されません。*以下のテキストをフッタとして使用*チェックマークを有効化して、フッタテキストを入力します。設定を保存するには*適用*をクリックします。

注 – メールクライアント(例: Microsoft Outlook または Mozilla Thunderbird)が署名済みまたは暗号化済みのメッセージにフッタを追加すると、署名が破壊されて無効になります。デジタル署名をクライアント側で作成する場合は、ウイルス対策チェックフッタオプションを無効にしてください。ただし、メール通信のプライバシーや認証を保ちながら、一般的なウイルス対策チェックフッタを使用する場合は、Sophos UTM の組み込みメール暗号化機能の使用を考慮してください。ゲートウェイ上でのメール暗号化では、デジタル署名を作成する前にフッタがメッセージに付加されるため、署名が損なわれることはありません。

10.1.4 スパム対策

Sophos UTMを設定して、未承諾のスパムメールを検出したり、既知の(または疑わしい)スパム発信者からのスパム送信を特定することができます。*スパム対策*タブにある設定オプションを使用して、SMTPのセキュリティ機能を設定し、未承諾の宣伝用メールなどからネットワークを保護します。

注 – 送信メールは、*リレー*タブの *リレー(送信) メッセージのスキャン*が選択されている場合にスキャンされます。

注 – このタブの機能の一部は、ベーシックガードサブスクリプションでは使用できません。

SMTPトランザクション中のスパム検知

SMTPトランザクション中にスパムを拒否することができます。*SMTP上でリジェクト*オプションに、次のいずれかの設定を選択します。

- *オフ*: スパム検出は無効となり、スパムが原因でメールが拒否されることは一切ありません。
- **Confirmed Spam**: 確認されたスパムのみ拒否されます。
- **Spam**: システムがスパムとみなす全てのメールが拒否されます。ニュースレターなどのメールを、スパムの疑いがあるとみなして却下する場合もあるため、誤検出率が高くなる可能性があります。

SMTPトランザクション中に拒否されないメールは、下の *スパムフィルタ*セクションに従って処理されます。

プロファイル モード:この設定はプロファイルごとには変更できません。メッセージが複数の受信者宛てであり、いずれかの受信者のプロファイルでスパムのスキャンが完全にオフになっている場合、この機能は省略されます。つまり、通常のスパムスキャン設定を*Spam*または*Confirmed Spam*のいずれかにしておくことをお勧めします。

RBLs (Realtime Blackhole Lists)

リアルタイムブラックホール リスト(RBL)とは、スパム行為に関連しているIPアドレスのリストをインターネットサイトが公開する方式です。

推奨RBLを使用:このオプションを選択すると、メール転送エージェントは外部のデータベースに対して既知のスパム送信者(いわゆる*リアルタイムブラックホール リスト*)を問い合わせます。あるサイトが、それらのリストの1つ以上に含まれていれば、このサイトからの送信メッセージを容易に拒否することができます。このようなサービスの一部はインターネットで利用できます。この機能を使用することにより、スパムを大幅に減らすことができます。
デフォルトで、以下のRBLに対して問い合わせます。

- Commtouch IP Reputation(ctipd.org)
- cbl.abuseat.org

注 –Sophos UTM が問い合わせるRBLリストは、予告なしに変更される場合があります。Sophosは、これらのデータベースの内容を保証しません。

Sophos UTMのスパム対策機能を強化するために、さらなるRBLサイトを追加して、スパム対策機能を強化できます。追加するには、*RBLゾーンの追加*ボックスでプラスアイコンをクリックします。表示されたテキストボックスにRBLゾーンを入力します。

設定を保存するには*適用*をクリックします。

スパムフィルタ

Sophos UTMには、スパムの特徴があるメールをヒューリスティックでチェックする機能があります。この機能は、SMTPエンベロープ情報と、ヒューリスティックテストおよび特性に関する内部データベースを使用します。このスパムフィルタオプションでは、メッセージの内容とSMTPエンベロープ情報に基づいてメッセージにスコアを付けます。スコアが高いほど、スパムの可能性が高いことを意味します。

次の2つのオプションを使用して、ある一定のスパムスコアが付いたメッセージへの対応方法を指定することができます。これにより、ゲートウェイはスパムの可能性があるメールを別個に扱うことができるようになります。

- *スパムアクション*: ここでは、スパムの可能性があるとして分類されたメッセージに対する対策を定義できます。ここでは、誤検出、つまり、ニュースレターなどが間違ってスパムに分類され、ブラックホール化によってメールが紛失する可能性があることに注意してください。
- *確実性の高いスパムへのアクション*: ここでは、確実性の高いスパムメッセージに対するアクションを定義できます。

これら2種類のスパムに対する処理を、さまざまな対策から選択できます。

- *オフ*: メッセージはスパムとしてマークされたり、フィルタされません。
- *警告*: メッセージはフィルタされません。受信メッセージの場合は、その代わりに、スパムフラグがメッセージヘッダに追加され、スパムマーカがメッセージの件名に追加されます。送信メッセージは、アクションなしで送信されます。
- *隔離*: メッセージはブロックされ、メールの隔離場所に保存されます。隔離されたメッセージは、ユーザポータルまたはデイリーの隔離レポートで確認できます。
- *ブラックホール*: メッセージは受信後、ただちに削除されます。送信メッセージは、意図しないメールの紛失を回避するために、ブラックホール化されることがありません。代わりに、隔離されます。

スパムマーカ: このオプションで、スパムマーカを指定できます。スパムマーカとは、スパムメッセージをすばやく簡単に識別できるように、メッセージの件名行に追加される文字列です。デフォルトでは、スパムメッセージを示すために `*SPAM*` という文字列が使用されます。

送信者ブラックリスト

受信SMTPセッションのエンベロープ送信者は、このブラックリスト内のアドレスと照合されます。エンベロープ送信者がブラックリストに含まれている場合、メッセージはSMTP上でリジェクトされます。*SMTP上でリジェクト*フィールドの設定は、この機能から影響を受けることはありません。
ブラックリストに新しいアドレスパターンを追加するには、*ブラックリストアドレスパターン*ボックスでプラスアイコンをクリックし、アドレス(の一部)を入力してから、*適用*をクリックします。ワイルドカードとしてアスタリスク(*)を使用できます(例: `*@abbeybnknational.com`)。

> ヒント – エンドユーザは、ユーザポータルで独自のメールホワイトリストとブラックリストを作成することができます。

表現フィルタ

表現フィルタは、SMTPプロキシを通過するメッセージに特定の表現が含まれていないか、コンテンツをスキャンし、疑わしいメールはブロックされます。表現は*Perl互換の正規表現*で指定できます。たとえば、「online dating」などの簡単な文字列は、大文字と小文字を区別しないで解釈されます。設定を保存するには*適用*をクリックします。

クロスリファレンス – 表現フィルタでの正規表現の使用に関する詳細情報は、SophosKnowledgebaseを参照してください。

スパム対策詳細機能

このエリアには、Sophos UTMのスパム対策機能を強化するその他のさまざまな詳細オプションがまとめられています。

無効なHELO/RDNS不可のリジェクト: 無効なHELOエントリを送信するホストやRDNSエントリが不足しているホストを拒否するには、このオプションを選択します。このチェックからホストを除外するには、*除外*タブを使用してください。

> **厳密なRDNSチェック**: 無効なRDNSレコードのホストからのメールを追加拒否するには、このオプションを選択します。RDNSレコードは、検出されたホスト名が元のIPアドレスに解決されない場合に無効になります。

グレイリスティング: グレイリスティングとは、基本的に、特定の期間にわたってメールを一時的に拒否することです。一般に、グレイリスティングを使用しているメールサーバは、すべての受信メールから3種類の情報を記録します。

- 送信者のアドレス
- メッセージ送信元のホストのIPアドレス
- 受信者のアドレス
- メッセージ件名

このデータセットは、SMTPプロキシの内部データベースと照合してチェックされます。新しいデータセットが見つかった場合には、それを記述する特別なタイムスタンプとともにデータベースに記録が作成されます。このデータセットにより、当該メールが5分間にわたって拒否されます。5分経つとプロキシがデータセットを認識します。当該メッセージが再送信されると、このメッセージは許可されます。データセットは、1週間以内に更新されなければ、1週間後に失効します。
グレイリスティングでは、ほとんどのスパムメッセージ送信者が「fire-and-forget」方式を使用している点を利用しています。これは「メールを送りつけて、うまくいかなければ忘れる」という方式です。つまり、RFC準拠のメールサーバと違い、スパムメール送信者は、一時的な失敗が発生したメールを再送信しません。この機能では、次のことが前提となっています。つまり、一時的な失敗はメール配信に関するRFC仕様に起因するため、正当なサーバは後でメールを再送信します。その時点で宛先にメールが受け入れられます。

BATVを使用: BATVとは、メールアドレスの正当な使用と不正な使用を区別することを目指すIETFのドラフトです。BATVは、簡単な共有鍵を追加してアドレス、時変情報、および任意のランダ

ムデータのハッシュを符号化することにより、送信メールのエンベロープ送信者に署名を施して、メールが本当に送信者からのものであると証明する方法を提供します。これは主に、送信者自身が送信したものではないバウンスメールを拒否するために使用されます。BATVを使用することにより、受信するバウンスが本当に自分が送信したEメールに由来しており、スパム送信者が偽造したアドレスからのメールではないことを確認できるようになります。戻ってきたバウンスメールのメールアドレスがBATVに従って署名されていない場合、SMTPプロキシはこのメッセージを受け付けません。BATVによる署名は7日後に失効します。メールのエンベロープ`MAIL FROM`アドレスのハッシュを符号化するために使用する鍵(別名*BATVシークレット*)を変更するには、*Eメールプロテクション* > *SMTP* > *詳細*タブに進みます。

注 – メール転送エージェントによっては、BATVによってエンベロープ送信者アドレスが変更されたメッセージを拒否する場合があります。この場合、影響を受ける送信者、受信者、ドメインに対して除外ルールを作成する必要があります。

チェックの実施:SPF(送信者ポリシフレームワーク:*Sender Policy Framework*)とは、ドメインの所有者が送信メールサーバに関する情報を公開するためのフレームワークです。ドメインは公開レコードを使用して、さまざまなサービス(Web、メールなど)をこれらのサービスを実行するマシンに送信します。すべてのドメインは、そのドメインへのメールをどのマシンが受信するのかを知らせるMXレコードをメール関連のサービス用に公開しています。SPFでは、ドメインからある種の「リバースMXレコード」を公開することにより、そのドメインからのメールを送信しているマシンを広く一般に伝えます。特定のドメインからメッセージを受信すると、受信者はそれらのレコードを確認して、正当な送信者からのメールであることを確認します。

クロスリファレンス- 詳細は、送信者ポリシフレームワークWebサイトでご確認ください。

追加のスパム対策機能として、SMTPプロキシは、任意のアドレスへのメールを受信したときに、バックエンドのメールサーバに対して受信者アドレスを暗黙でチェックしてからそのメールを受け付けます。無効な受信者アドレスへのEメールは許可されません。この機能が動作するためには、使用しているバックエンドメールサーバが、SMTPステージで不明受信者へのメールを拒否できなければなりません。原則的に、バックエンドサーバがメッセージを拒否すれば、SMTPプロキシもこのメッセージを拒否します。

ただし、受信者の確認は信頼される(許可される)ホストやリレーホストに対しては*行われません*。この理由は、ユーザエージェントによっては、SMTPトランザクションで受信者が拒否されると問題が発生する場合があるためです。一般的なシナリオ(バックエンドメールサーバがSMTPトランザクションで不明な受信者を拒否する)では、Sophos UTMバウンスが生成されるのは次の場合に限られます。

- 信頼される送信元やリレー元が、配信不能な受信者にメッセージを送信した場合。
- バックエンドメールサーバが停止しており、Sophos UTMが受信者を確認できなかった場合。

ただし、Sophos UTMは、バックエンドメールサーバからの配信不能レポート(NDR)やバウンスの送信を防止することはできません。さらにSophos UTMは、メールサーバからのスパムの可能性のあるコールアウト応答は24時間キャッシュし、可能性のないものは2時間キャッシュします。

10.1.5 データ保護

*SMTP > データ保護*タブでは、データ保護機能により、機密データを含むファイル転送のモニタリングや制限を行うことにより、ワークステーションからの偶発的なデータ損失を軽減することができます。偶発的なデータ損失は、一般的に従業員の機密データの取り扱いミスが原因となります。例:ユーザが家庭用のメール(SMTP)を経由して機密データを含むファイルを送信するなど。Data Protectionは件名、メッセージ本文、および機密情報の添付などを含む送信メールをスキャンします。結果に基づき、メールはSPX暗号化を使用して暗号化、またはメールの拒否もしくは送信することができます。

Data Protectionを設定するには、次のセクションで設定を定義します。Sophosコンテンツコントロールが選択されていないか、カスタムルールが定義されていない限り、この機能は無効です。

データ保護ポリシー

添付内をスキャン:これを選択すると、機密データに対する添付やさらにはメッセージ本文もスキャンされます。このスキャンはSAVIエンジンを使用して、現在のデータベースにより、非常にさまざまなファイルタイプをスキャンします。

ルールの一致におけるアクション:ポリシがトリガされている場合、メールを取り扱う方法として選択します。

ブラックホール:ポリシがトリガされているメールは送信されません。

SPX暗号化で送信:ポリシがトリガされているメールは自動的にSPX暗号化されて送信されます(*Eメールプロテクション > SPX暗号化*タブを参照)。SMTPがシンプルモードで使用される場合、*SMTP > とグローバル*タブで選択されたSPXテンプレートがSPX暗号化に使用されます。SMTPがプロファイルモードで使用される場合、送信者のドメインがアサインされているSMTPプロファイルに応じてSPXテンプレートが使用されます(*SMTPプロファイル*タブを参照)。送信者のドメインが任意のプロファイルに割り当てられていない場合、*SMTP > グローバル*タブで選択されたデフォルトのテンプレートが使用されます。

許可:ポリシがトリガされているメールである場合でも送信されます。

合致時の通知先：以下の人物に通知するかどうか選択します。

- メール送信者、
- 管理者、
- その他、
- または全員。

  その他の隣にメールアドレスを入力する必要があります。通知メールは、*管理* > *カスタマイズ* > *E メール メッセージ*タブでカスタマイズできます。

設定を保存するには*適用*をクリックします。

Sophos コンテンツ コントロール リスト ルール

タイプ：ドロップダウンリストからエントリを選択し、表示されるルールに応じて数を減らします。

地域：ドロップダウンリストからエントリを選択し、表示されるルールに応じて数を減らします。

選択したルールのみ表示：有効にすると、選択したルールのみがリストに表示されます。

ルール：Data Protection機能に使用するルールを選択します。エントリの上へカーソルを移動させると、ツールのヒントとともにルールに関する追加情報が表示されます。

設定を保存するには*適用*をクリックします。

カスタム ルール

*カスタム*表現：上記で選択したルールに加え、Data Protection機能で使用する表現を入力します。正規表現を追加することができます。

> *クロスリファレンス* – ここでの正規表現の使用に関する詳細情報は、SophosKnowledgebaseを参照してください。

設定を保存するには*適用*をクリックします。

10.1.6 除外

SMTP > *除外*タブで、アンチスパム、ウイルス対策、またはその他のセキュリティチェックから除外するホワイトリストのホスト、ネットワーク、送信者、および受信者を定義できます。

注 – メールは多数の受信者に送信される場合がありますが、Sophos UTMはSMTPプロトコルのインラインスキャニングを実装しているため、メール受信者のうち1人でも*受信者*ボックスにリストされていると、メールのスキャンはすべての受信者に対してスキップされます。

除外ルールを作成するには、次の手順に従います。

1. ***除外*タブで、*新規除外リスト*をクリックします。**
   *除外リストを追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前: この除外ルールを説明する名前を入力してください。

   実行しないチェック: スキップするセキュリティチェックを選択します。詳細は、*Eメールプロテクション > SMTP > ウイルス対策*および*スパム対策*を参照してください*データ保護*。

   送信元ホスト/ネットワークで除外: この除外ルールで定義されたセキュリティチェックをスキップする送信元ホスト/ネットワーク(メッセージが発信されたホストまたはネットワーク)を選択または追加します。定義を追加する方法は、*定義とユーザ > ネットワーク定義 > ネットワーク定義*ページで説明しています。

   注 – ローカルメッセージはデフォルトでスキャンされないので、ローカルホストには除外を作成する必要はありません。

   このオプションを選択すると、*ホスト/ネットワーク*ボックスが開きます。「+」アイコンまたはフォルダアイコンをクリックして、ホストあるいはネットワークを追加できます。

   または これらの送信者アドレス: 定義されたセキュリティチェックをスキップする送信者のEメールアドレスを選択します。

   このオプションを選択すると、*送信者*ボックスが開きます。完全で有効なメールアドレスを入力するか(例:`jdoe@example.com`)、またはアスタリスクをワイルドカードとして使用して特定ドメインのすべてのメールアドレスを指定できます(例:`*@example.com`)。

   注 – 送信者アドレスは容易に偽造できるため、*送信者*オプションを使用する際は注意が必要です。

   または これらの受信者アドレス: 定義されたセキュリティチェックをスキップする受信者のEメールアドレスを選択します。

このオプションを選択すると、*受信者*ボックスが開きます。完全で有効なメールアドレスを入力するか(例:`jdoe@example.com`)、またはアスタリスクをワイルドカードとして使用して特定ドメインのすべてのメールアドレスを指定できます(例:`*@example.com`)。

コメント(オプション):説明などの情報を追加します。

3. ***保存*をクリックします。**
新しい除外ルールが*除外*リストに表示されます。

除外ルールを編集または削除するには、対応するボタンをクリックします。

10.1.7 リレー

SMTPプロキシはメールリレーとして使用できます。メールリレーは、特定のユーザ、ユーザグループ、あるいはホストがそれを介してローカル以外のドメインにメールをリレー(送信)できるように設定されたSMTPサーバです。

注 – このタブの機能の一部は、ベーシックガードサブスクリプションでは使用できません。

アップストリームホストリスト

アップストリームのホストは、メールをお客様のISPあるいは外部MXに転送するホストです。スタティックなアップストリームのホストからメールを受信する場合は、ここにホストを入力する必要があります。ホストを入力しないと、スパム保護が正常に機能しなくなります。

アップストリームホストを追加するには、「+」アイコンまたはフォルダアイコンをクリックして、*ネットワーク*オブジェクトリストからドラッグ&ドロップします。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。アップストリームホストのみを許可する場合は、*アップストリーム/リレーホストのみ許可*チェックボックスにチェックを入れます。これにより、SMTPアクセスは、定義されたアップストリームホストに制限されます。アップストリームホストは、リレー特権の取得を認証できます。設定を保存するには*適用*をクリックします。

認証リレー

SMTPクライアントは、リレー特権の取得を認証できます。*認証によるリレーの許可*チェックボックスにチェックを入れて、この機能を使用できるようにするユーザおよびユーザグループを指定します。ユーザを追加する方法は、*定義とユーザ* > *ユーザとグループ* > *ユーザ*ページで説明しています。設定を保存するには*適用*をクリックします。

注 – *アップストリーム/リレーホストのみ許可*チェックボックスにチェックが入っている場合、*認証リレー*は送信ホストがアップストリーム/リレーホストとして設定されている場合にのみ機能します。

ホストベースリレー

メールリレーも、ホストベースに対応できます。お使いのローカルメールサーバあるいはメールクライアントがSMTPプロキシをメールリレーとして使用する必要がある場合は、リレーを介してメールを送信できるようにするネットワークやホストを*許可ホスト/ネットワーク*ボックスに追加する必要があります。リストされたネットワークやホストは、どのアドレスにもメッセージを送信できます。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

警告 – *許可ホスト/ネットワーク*ボックスでは、絶対に*すべて*を選択しないでください。これを選択すると、オープンリレーになり、インターネット上の誰もがSMTPプロキシ経由でメッセージを送信できるようになります。スパム送信者はこれをすぐに見つけ、大量のメールトラフィックを送信します。最悪の場合は、お客様がサードパーティのスパマーブラックリストに載ることになってしまいます。ほとんどの設定では、お客様のネットワークのメールサーバだけを、メールのリレーを許可される唯一のホストとすべきです。

設定を保存するには*適用*をクリックします。

ホスト/ネットワークのブラックリスト

ここで、SMTPプロキシでブロックするホストおよびネットワークを定義できます。設定を保存するには*適用*をクリックします。

リレー(送信)メッセージ

このオプションを有効にすると、認証されたリレーあるいはホストベースのリレーで送信されるメッセージについて、悪意あるコンテンツの有無がスキャンされます。送信メールが大量にある場合、このオプションをオフにすると、パフォーマンスが向上します。設定を保存するには*適用*をクリックします。

送信メッセージには、グローバルなウイルス対策およびアンチスパム設定も適用されます。ただし、これらの設定を問わず、感染メッセージやスパムメッセージはブラックホール化ではなく常に隔離されます。これにより、意図しないメールの紛失が回避されます。

10.1.8 詳細

*SMTP > 詳細*タブでは、スマートホストの設定や透過モードスキップリストなどのSMTPプロキシの追加セキュリティオプションを設定できます。

ヘッダ変更

UTMを通過するEメールのSMTPヘッダコンテンツは、*ヘッダ変更*で変更および/または削除できます。

ヘッダを追加/削除するには:

1. **「+」アイコンをクリックします。**
   *ヘッダ変更ルールの追加*ダイアログが開きます。

2. **要求の*オペレーション*選択します。**

3. **変更/削除する*ヘッダ名*を入力します。**
   1～255のASCII文字を使用できます。

4. **ヘッダを追加する場合、新しいヘッダが持つべき*値*を入力します。**
   0～255文字を使用できます。

5. **必要に応じて*コメント*を追加します。**

6. ***保存*をクリックします。**

7. ***適用*をクリックします。**
   設定が保存されます。

ヘッダルールを編集または削除するには、当該ルールの横のアイコンをクリックします。

透過モード

SMTPの透過モードを有効にするには、チェックボックスにチェックを入れ、*適用*をクリックします。*透過モード時にスキップするホスト/ネット*ボックスにリストされているホストとネットワークは、SMTPトラフィックの透過的インターセプションの対象とはなりません。ただし、これらのホストおよびネットワークでSMTPトラフィックを許可するには、*リスト内のホスト/ネットワークのSMTPトラフィックを許可*チェックボックスにチェックを入れます。このチェックボックスにチェックを入れない場合は、ここでリストされているホストとネットワークに特定のファイアウォールルールを定義する必要があります。設定を保存するには*適用*をクリックします。

TLS設定

TLS証明書:ドロップダウンリストから証明書を選択します。この証明書は、TLS証明書は、*サイト間 VPN > 証明書管理 > 証明書*タブで作成またはアップロードできます。暗号化についてそれをサポートしているすべてのリモートホストとネゴシエートするために使用されます。

TLSネゴシエーション必須のホスト/ネット:ここに、メール通信のTLS暗号化が常に必要なホストまたはネットを追加または選択します。これにより、UTMは、これらのホスト/ネットで何らかの理由でTLS暗号化を使用できない場合に、メールを抑制します。つまり、TLSが使用可能になるまで、メッセージはメールキューに保留されます。一定の期間にわたってTLSを使用できない場合は、送信の試行が停止され、メールを送信できなかったという通知がユーザに送信されます。

TLSネゴシエーション必須の送信ドメイン:特定のドメインに対して受信メールのTLS暗号化を強制するには、ここにドメインを入力します。これらのドメインからTLSなしで送信されたメールは、即時に拒否されます。

TLSネゴシエーションをスキップするホスト/ネット:特定のホストやネットワークでTLS暗号化に関する問題が発生した場合は、それをボックスに入力し、適切なTLS証明書をドロップダウンメニューから選択します。それによって、UTMは、このホストまたはネットワークに対するTLSネゴシエーションをスキップします。設定を保存するには*適用*をクリックします。

DomainKeys Identified Mail (DKIM)

DKIMは発信メッセージに暗号によって署名する方法です。DKIM署名を使用するには、RSA鍵と対応する鍵セレクタを各フィールドに入力し、メールに署名するドメインを*DKIM ドメイン*ボックスに追加します。設定を保存するには*適用*をクリックします。

機密性表明フッタ

各送信メールについて、メールに機密情報や部外秘の情報が含まれていることなどをユーザーに知らせる、機密フッタを追加してカスタマイズできます。さらに、機密フッタは、メールが返信の場合 *In-Reply-To*ヘッダを持つもの)またはメールのコンテンツタイプを判定できない場合は、メールに追加されません。

注 – メールクライアント(例: Microsoft Outlook または Mozilla Thunderbird)が署名済みまたは暗号化済みのメッセージにフッタを追加すると、署名が破壊されて無効になります。デジタル署名をクライアント側で作成する場合は、ウイルス対策チェックフッタオプションを無効にしてください。ただし、メール通信のプライバシーや認証を保ちながら、一般的なウイルス対策チェックフッタを使用する場合は、Sophos UTM の組み込みメール暗号化機能の使用を考慮してください。

メール暗号化では、デジタル署名を作成する前にフッタがメッセージに付加されるため、署名が損なわれることはありません。

詳細設定

ここで、SMTPホスト名やポストマスタアドレスなどを設定できます。

SMTPホスト名 : SMTPホスト名を設定すると、プロキシは、HELOおよびSMTPバナーメッセージで指定された名前を使用します。デフォルトでは、通常システムのホスト名が選択されています。

Postmasterアドレス: 送信されたメッセージの転送先となるUTMのポストマスタのメールアドレスを`postmaster@[192.168.16.8]`の形で指定します。この場合、IPリテラルアドレスが、UTMのIPアドレスの1つになります。そのようなメッセージを受け入れることがRFC要件となっています。

BATVシークレット: ここで、SMTPプロキシが使用する、自動的に生成されたBATVシークレットを変更できます。BATVシークレットはメールのエンベロープの`MailFrom`アドレスへの署名に使用される共有鍵で、無効なバウンスアドレスの検出を可能にします。複数のMXをドメインに使用している場合は、BATVシークレットをすべてのシステムで同じものに変更できます。

最大メッセージサイズ: プロキシが受け付ける最大メッセージサイズ。この設定は送受信両方のメールに適用されます。バックエンドサーバにメッセージサイズの制限がある場合は、ここではその制限値以下に設定する必要があります。

最大コネクション数 : プロキシが許可する最大同時接続数。デフォルトは20です。

最大コネクション数/ホスト: プロキシが許可する1ホスト当たりの最大コネクション数。デフォルトは10です。

最大メール数/コネクション: プロキシが許可するコネクションあたりの最大メール数。バッファサイズはバッファに保持されるログの行数です。

最大受信者/メール: プロキシが許可するメールあたりの最大受信者数。デフォルトは100です。

フッタモード: ここでメールへのフッタの追加方法を定義できます。*MIMEパート*を指定すると、追加のMIMEパートとしてフッタを追加します。既存のパートエンコーディングは変更されないので、元の文字コードが保持されます。別の方式である*インライン*では、フッタがメール本体から区切り記号--で分離されます。このモードでは、フッタでUnicode(UTF-8)変換を使用するかどうかを選択できます。Unicode変換を行うと、フッタで元の文字コードを保持するようにメッセージがアップグレードされます。

スマートホスト設定

スマートホストはメールリレーサーバの一種で、SMTPサーバが受信者のサーバに直接メールをルーティングするのではなく、アップストリームのメールサーバにルーティングできるようにします。多くの場合このスマートホストは、送信者がスマートホストを通してメールを送信する権限を持つことを確認するために、送信者の認証を必要とします。

スマートホストを使用：メールの送信にスマートホストを使用する場合は、このチェックボックスにチェックを入れます。このオプションを選択すると、プロキシ自体がメールを配信することはなくなり、すべてをスマートホストに送信するようになります。

- スマートホスト：スマートホストオブジェクトを選択または追加します。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。
- スマートホストポート：スマートホスト接続のデフォルトポートは25です。必要に応じて、ポートを変更できます。
- スマートホスト認証が必要：スマートホストが認証を必要とする場合は、チェックボックスにチェックを入れます。*プレーン*と*ログイン*認証タイプの両方がサポートされています。それぞれのフィールドにユーザ名とパスワードを入力します。

10.2 SMTPプロファイル

Sophos UTMのSMTPプロキシで、別のSMTPプロファイルを作成し、それを異なるドメインに関連付けることができます。このようにして、*Eメールプロテクション* > *SMTP*で設定されたデフォルトのプロファイル以外のプロファイルを使用する特定のドメインを指定できます。機能の順序はタブによって構造化され、SMTPトランザクション時に各ステップが互いにどのように処理されるかを決定します。

SMTPプロファイルを作成するには、以下の手順に従います。

1. **SMTPプロファイルモードを有効にします。**
   Eメールプロテクション > *SMTP* > *グローバル*タブで、*プロファイルモード*を選択して*適用*をクリックします。

   Eメールプロテクション > *SMTPプロファイル*メニューのSMTPプロファイル作成が有効になります。

2. ***SMTP プロファイル*タブで、*新規プロファイル*をクリックします。**
   ダイアログボックスが開きます。

3. プロファイルを説明する名前を入力してください。

4. **1つ以上のドメインを追加します。**
 1つ以上のドメインを*ドメイン*ボックスに追加します。

 このプロファイルの設定が、それらのドメインに適用されます。

5. **次の設定を行います。**
 使用する機能にのみ設定します。以下の各機能に対して、ここで定義する個々の設定を使用するか、または*Eメールプロテクション* > *SMTP*で定義するグローバル設定を使用するかを決定できます。デフォルトでは、グローバル設定オプションが選択されています。各機能の個々の設定について以下に説明します。

 注 – ここで設定されたドメイン名が送信者アドレスに含まれる暗号化されたメールは、Sophos UTMのメール暗号化/復号化エンジンを使用しても復号化できません。したがって、外部メールドメインのプロファイルは含めないようにしてください。

 ここで定義できるすべての設定は、*Eメールプロテクション* > *SMTP*でもグローバルに設定できます。したがって、ここでは、設定の一覧とグローバル設定との相違点のみを、対応するグローバル設定へのクロスリファレンスとともに示します。設定の詳細は、グローバル設定でご覧ください。

 以下の設定を行うことができます。

 - ルーティング: *ルーティング*タブで、SMTPプロキシのドメインとルーティングターゲットを設定し、受信者の検証方法を定義します。

   - スタティックホストリスト
   - DNSホスト名
   - MXレコード

   詳細は、*Eメールプロテクション* > *SMTP* > *ルーティング*を参照してください。

 - 受信者検証

   受信者検証: ここでメール受信者を確認するかどうかと確認方法を指定できます。

   - コールアウト使用: 受信者検証の要求がサーバに送信されます。
   - **Active Directory**: 受信者検証の要求がActive Directoryサーバに送信されます。Active Directoryを使用するには、*定義とユーザ* > *認証サービス* > *サーバ*で指定されたActive Directoryサーバを備えていることが必要です。ベースDNを*代替ベースDN*フィールドに入力します。

> 注 – Active Directory 受信者検証を使用すると、サーバーが応答しない場合にメッセージがバウンスされる場合があります。

- オフ: 受信者確認は完全にオフにできますが、推奨されません。なぜなら、オフにすると、スパムトラフィックが増大して、辞書攻撃の危険性が高まるからです。この結果、隔離場所が迷惑メールで溢れてしまうことになります。

詳細は、*Eメールプロテクション > SMTP > ルーティング*を参照してください。

- **Sophos UTM RBLs**: ここでスパムにリンクしたIPアドレスをブロックできます。
  - 推奨RBLを使用

  詳細は、*Eメールプロテクション > SMTP > スパム対策*を参照してください。

- 追加**RBL**: さらなるRBLサイトを追加して、Sophos UTMのスパム対策機能を強化できます。詳細は、*Eメールプロテクション > SMTP > スパム対策*を参照してください。3番目のオプションとして、ここで個別の設定にグローバル設定を追加できます。

- **BATV/RDNS/HELO/SPF/**グレーリスト化: このタブでは、Sophos UTMのアンチスパム機能を強化するために、次のような他のさまざまな高度なオプションを使用できます。
  - 無効なHELO/RDNS不可のリジェクト
  - グレイリスティングを使用
  - BATVを使用
  - SPFチェックの実施

  詳細は、*Eメールプロテクション > SMTP > スパム対策*を参照してください。

- ウイルス対策 スキャン: 悪意あるコンテンツを含むメッセージの処理方法を設定できます。次の作業を実行できます。
  - オフ
  - 隔離
  - ブラックホール

  以下のアンチウイルススキャンオプションから選択できます。

  - シングルスキャン: デフォルト設定。*システム設定 > スキャン設定*タブに定義されたエンジンを使用して最高レベルのパフォーマンスを実現します。

- デュアルスキャン: 各トラフィックに対し、異なるウイルススキャナを使用してスキャンを2回行うことにより、検知率を最大限に高めます。デュアルスキャンは、ベーシックガードサブスクリプションでは使用できません。

  スキャンできないコンテンツ、暗号化されたコンテンツの隔離: このオプションを選択して、コンテンツをスキャンできなかったメールを隔離します。スキャンできないコンテンツは、暗号化されたもの、破損したアーカイブ、またはサイズが大きすぎるコンテンツの他、スキャナの不具合などの技術的な問題による場合があります。

  詳細は、*Eメールプロテクション > SMTP > ウイルス対策*を参照してください。

- スパム対策スキャン: ここで迷惑な宣伝メールの取り扱いを決めます。スパムおよびスパムと確認されたメールに対して以下の対策を選択できます。
  - オフ
  - 警告
  - 隔離
  - ブラックホール

  詳細は、*Eメールプロテクション > SMTP > スパム対策*を参照してください。

- 送信者ブラックリスト: 受信SMTPセッションのエンベロープ送信者は、このブラックリスト内のアドレスと照合されます。エンベロープ送信者がブラックリストに含まれている場合、メッセージはブラックホール化されます。詳細は、*Eメールプロテクション > SMTP > スパム対策*を参照してください。3番目のオプションとして、ここで個別の設定にグローバル設定を追加できます。

- **MIME**音声/動画/実行可能ファイルのブロック: MIMEタイプのフィルタはMIMEタイプのEメールコンテンツを読みます。どのタイプのコンテンツを隔離するかを選択できます。
  - オーディオコンテンツ
  - ビデオコンテンツ
  - 実行形式コンテンツ

  詳細は、*Eメールプロテクション > SMTP > ウイルス対策*を参照してください。

- **MIME**タイプブラックリスト: ここで、その他のMIMEタイプを隔離場所(検疫)に追加できます。詳細は、*Eメールプロテクション > SMTP > ウイルス対策*を参照してください。3番目のオプションとして、ここで個別の設定にグローバル設定を追加できます。

- **MIME**タイプホワイトリスト: ここで隔離しないMIMEタイプを追加できます。詳細は、*Eメールプロテクション > SMTP > ウイルス対策*を参照してください。3番目のオプションとして、ここで個別の設定にグローバル設定を追加できます。
- ブロック対象ファイル拡張子: *ファイル拡張子フィルタ*を使用して、ファイル拡張子に基づいて、特定のファイルタイプ（例：実行可能ファイル）を含むメールを（警告付きで）隔離できます。詳細は、*Eメールプロテクション > SMTP > ウイルス対策*を参照してください。3番目のオプションとして、ここで個別の設定にグローバル設定を追加できます。
- ブロック対象表現: 表現フィルタは、SMTPプロキシを通過するメッセージに特定の表現が含まれていないか、コンテンツをスキャンし、疑わしいメールはブロックされます。疑わしいメールはブロックされます。詳細は、*Eメールプロテクション > SMTP > スパム対策*を参照してください。3番目のオプションとして、ここで個別の設定にグローバル設定を追加できます。
- 機密性表明フッタ: 各送信メールについて、メールに機密情報や部外秘の情報が含まれていることなどをユーザーに知らせる、機密フッタを追加してカスタマイズできます。さらに、機密フッタは、メールが返信の場合 *In-Reply-To*ヘッダを持つもの）またはメールのコンテンツタイプを判定できない場合は、メールに追加されません。送信者ドメインに応じて、フッタが追加されます。フッタを使用するには、チェックボックスにチェックを入れ、フッタのテキストを入力します。
- **SPX** テンプレートの選択: SPXテンプレートはSPXの暗号化に使用されます。暗号化されたメールを受信者に送信する方法を定義します。詳細は、*Eメールプロテクション > SPX暗号化 > SPXテンプレート*を参照してください。
- データ保護設定: ここでスキャンリストへの添付の追加、通知の設定、および*SophosLabs コンテンツコントロールリスト*から項目を選択することができます。

  詳細は、*SMTP > データ保護*を参照してください。

6. *適用***をクリックします。**
   設定が保存されます。新しいプロファイルが*SMTPプロファイル*リストに表示されます。

注 – トピックに*グローバル設定の使用*を選択して*適用*をクリックすると、機能のアイコンがグローバル設定のアイコンに変わります。これにより、どの機能に対してグローバル設定または個々の設定が適用されているかが簡単にわかります。

プロファイルの無効化、名前変更、または削除を行う場合は、プロファイルドロップダウンリスト下にある上段の該当するボタンをクリックします。

10.3 POP3

Eメールプロテクション > *POP3*メニューでは、受信メールのPOP3プロキシを設定できます。*Post Office Protocol 3*(POP3)はアプリケーション層インターネット標準プロトコルで、リモートメールサーバーからのメールの取り出しを可能にします。POP3プロキシは透過的に機能します。つまりポート 110 または 995(TLSによる暗号化)で内部ネットワークから受信するすべての POP3 要求は、クライアントには認識されずにプロキシを通して傍受され、リダイレクトされます。このモードのメリットは、その他の管理やクライアント側の設定が必要ないということです。

注 – 場合によっては、メールクライアントの設定でサーバータイムアウト設定を長くすることが必要です。通常のデフォルトである約 1分以内の設定では、特に大きなメールをフェッチするときには短すぎます。

POP3プロトコルには、どのメールがすでに取り出されたかをサーバー側で追跡する機能はありません。一般的には、メールクライアントがメールを取り出した後、サーバー上でそれを削除します。ただし、クライアントがメールを削除しないように設定されている場合、サーバー側の削除は行われず、どのメールがすでにフェッチされたかをクライアントが追跡します。

10.3.1 グローバル

Eメールプロテクション > *POP3* > *グローバル*タブでは、POP3プロキシの基本設定を構成できます。

POP3プロキシを設定するには、以下の手順に従います。

1. **POP3プロキシを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、*POP3設定*エリアが編集可能になります。

2. **許可するネットワークを選択します。**
   プロキシPOP3トラフィックに許可するネットワークを追加または選択します。通常は、これは内部ネットワークです。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

   警告 – セキュリティリスクを招き、インターネットの悪用に道を開くので、決してネットワークオブジェクトで*すべて*を選択しないでください。

3. *適用*をクリックします。
   設定が保存されます。

   トグルスイッチが緑色に変わります。
設定をキャンセルするには、アンバー色のトグルスイッチをクリックします。

ライブログ

*POP3 ライブログ*は、POP3プロキシのアクティビティをログし、すべての受信メールを表示します。ボタンをクリックして、新しいウィンドウでライブログを開きます。

10.3.2 ウイルス対策

*ウイルス対策*タブには、ウイルス、ワーム、その他のマルウェアなどの有害で危険なコンテンツを含むメールに対するさまざまな対策が含まれています。

ウイルス対策スキャン

このオプションでは、ウイルス、トロイの木馬、疑わしいファイルタイプなどの不要なコンテンツがないかどうか、メールをスキャンします。悪意のあるコンテンツを含むメッセージはブロックされて、メールの隔離場所に保存されます。ユーザは、Sophos ユーザポータルまたはデイリーの隔離レポートで、隔離されたメッセージを確認してリリースできます。ただし、悪意のあるコンテンツを含むメッセージは、メールマネージャで管理者のみが隔離からリリースできます。

Sophos UTMは、最高のセキュリティを実現するさまざまなウイルス対策エンジンを備えています。

- シングルスキャン: デフォルト設定。*システム設定* > *スキャン設定*タブに定義されたエンジンを使用して最高レベルのパフォーマンスを実現します。
- デュアルスキャン: 各トラフィックに対し、異なるウイルススキャナを使用してスキャンを2回行うことにより、検知率を最大限に高めます。デュアルスキャンは、ベーシックガードサブスクリプションでは使用できません。

スキャンできないコンテンツ、暗号化されたコンテンツの隔離: このオプションを選択して、コンテンツをスキャンできなかったメールを隔離します。スキャンできないコンテンツは、暗号化されたもの、破損したアーカイブ、またはサイズが大きすぎるコンテンツの他、スキャナの不具合などの技術的な問題による場合があります。

最大スキャンサイズ: ウイルス対策エンジンでスキャンする最大ファイルサイズを指定します。このサイズを超えるファイルはスキャン対象外となります。

設定を保存するには*適用*をクリックします。

ファイル拡張子フィルタ

この機能は、ファイル拡張子に基づいて特定タイプのファイル(実行可能ファイルなど)を含むメールを(警告付きで)フィルタリングし、隔離します。ファイル拡張子を追加するには、*ブロック対象ファイル拡張子*ボックスの「+」アイコンをクリックし、スキャンするファイル拡張子(例: `exe` または `jar` (区切り文字のドットなし))を入力します。設定を保存するには*適用*をクリックします。

注 – 禁止されているファイル拡張子について、アーカイブはスキャンされません。アーカイブに含まれるマルウェアからネットワークを保護するために、アーカイブのファイル拡張子をすべてブロックすることを検討してください。

10.3.3 スパム対策

Sophos UTMを設定して、未承諾のスパムメールを検出したり、既知の(または疑わしい)スパム発信者からのスパム送信を特定することができます。*スパム対策*タブにある設定オプションを使用して、POP3のセキュリティ機能を設定し、未承諾の宣伝用メールなどからネットワークを保護します。

スパムフィルタ

Sophos UTMには、スパムの特徴がある受信メールをヒューリスティックにチェックする機能があります。この機能は、SMTPエンベロープ情報と、発見的テストおよび特性に関する内部データベースを使用します。このスパムフィルタオプションでは、メッセージの内容とSMTPエンベロープ情報に基づいてメッセージにスコアを付けます。スコアが高いほど、スパムの可能性が高いことを意味します。

次の2つのオプションを使用して、ある一定のスパムスコアが付いたメッセージへの対応方法を指定することができます。これにより、ゲートウェイはスパムの可能性があるメールを別個に扱うことができるようになります。

- *スパムアクション*: ここでは、スパムの可能性があるとして分類されたメッセージに対する対策を定義できます。
- *確実性の高いスパムへのアクション*: ここでは、確実性の高いスパムメッセージに対するアクションを定義できます。

これら2種類のスパムに対する処理を、さまざまな対策から選択できます。

- オフ: メッセージはスパムとしてマークされたり、フィルタされません。
- 警告: メッセージはフィルタされません。その代わりに、スパムフラグがメッセージヘッダに追加され、スパムマーカがメッセージの件名に追加されます。
- 隔離: メッセージはブロックされ、メールの隔離場所に保存されます。隔離されたメッセージは、ユーザポータルまたはデイリーの隔離レポートで確認できます。

スパムマーカ: このオプションで、スパムマーカを指定できます。スパムマーカとは、スパムメッセージをすばやく簡単に識別できるように、メッセージの件名行に追加される文字列です。デフォルトでは、スパムメッセージを示すために `*SPAM*` という文字列が使用されます。

表現フィルタ

表現フィルタは、特定の表現を探してメッセージの件名や本文をスキャンします。ここにリストされた表現を含むメールはブロックされます。ただし、*Eメールプロテクション > POP3 > 詳細*タブでプリフェッチオプションが有効になっている場合は、メールは隔離場所に送られます。表現は*Perl互換の正規表現*で指定できます。たとえば、「online dating」などの簡単な文字列は、大文字と小文字を区別しないで解釈されます。

クロスリファレンス – 表現フィルタでの正規表現の使用に関する詳細情報は、SophosKnowledgebaseを参照してください。

設定を保存するには*適用*をクリックします。

送信者ブラックリスト

受信するPOP3セッションのエンベロープの送信者が、このブラックリストのアドレスと照合されます。エンベロープの送信者がブラックリストにある場合、メッセージは隔離され、件名行に*Other*とマークされます。
ブラックリストに新しいアドレスパターンを追加するには、*ブラックリストアドレスパターン*ボックスでプラスアイコンをクリックし、アドレス(の一部)を入力してから、*適用*をクリックします。ワイルドカードとしてアスタリスク(*)を使用できます(例: `*@abbeybnknational.com`)。

ヒント – エンドユーザは、ユーザポータルで独自のメールホワイトリストとブラックリストを作成することができます。

10.3.4 除外

*POP3 > 除外*タブで、さまざまなセキュリティ機能から除外するクライアントホスト/ネットワークや送信者アドレスを定義できます。

除外ルールを作成するには、次の手順に従います。

1. ***除外*タブで、*新規除外リスト*をクリックします。**
   *除外リストを追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:この除外ルールを説明する名前を入力してください。

   実行しないチェック:スキップするセキュリティチェックを選択します。詳細は、*Eメールプロテクション > POP3 > ウイルス対策*および*ウイルス対策*を参照してください。

   クライアントホスト/ネットワークで除外:セキュリティチェックをスキップする送信元ホスト/ネットワーク(メッセージを発信したホストまたはネットワーク)を追加または選択します。定義を追加する方法は、*定義とユーザ > ネットワーク定義 > ネットワーク定義*ページで説明しています。

   注 – ローカルメッセージはデフォルトでスキャンされないので、ローカルホストには除外を作成する必要はありません。

   このオプションを選択すると、*クライアントホスト/ネットワーク*ダイアログボックスが開きます。「+」記号またはフォルダ記号をクリックして、ホストあるいはネットワークを追加できます。

   または これらの送信者アドレス:定義されたセキュリティチェックをスキップする送信者のEメールアドレスを選択します。

   このオプションを選択すると、*送信者*ボックスが開きます。完全で有効なメールアドレスを入力するか(例:`jdoe@example.com`)、またはアスタリスクをワイルドカードとして使用して特定ドメインのすべてのメールアドレスを指定できます(例:`*@example.com`)。

   注 – 送信者アドレスは容易に偽造できるため、*送信者*オプションを使用する際は注意が必要です。

   コメント(オプション):説明などの情報を追加します。

3. ***保存*をクリックします。**
   新しい除外ルールが*除外*リストに表示されます。

除外ルールを編集または削除するには、対応するボタンをクリックします。

10.3.5 詳細

*POP3 > 詳細*タブで、POP3プロキシの透過モードをスキップできるホストとネットワークを指定できます。さらに、このタブには、POP3プロキシのプリフェッチオプションが含まれています。プリフェッチオプションにより、POP3サーバからメッセージをプリフェッチ（事前取得）してデータベースに保存できます。

透過モードスキップリスト

*透過モード時にスキップするホスト/ネット*ボックスにリストされているホストとネットワークは、POP3トラフィックの透過的インターセプションの対象とはなりません。ただし、これらのホストおよびネットワークでPOP3トラフィックを許可するには、*リスト内のホスト/ネットワークのPOP3トラフィックを許可*チェックボックスにチェックを入れます。このチェックボックスにチェックを入れない場合は、ここでリストされているホストとネットワークに特定のファイアウォールルールを定義する必要があります。

POP3サーバとプリフェッチ設定

ネットワークまたはエンドユーザが使用するため、プロキシが認識できるように、ここに1つ以上のPOP3サーバを入力します。さらに、プリフェッチをオンにできます。

POP3サーバを指定するには、次の手順に従います。

1. **POP3サーバのDNS名を追加します。**
   *POP3サーバ*ボックスで、「+」アイコンをクリックします。*サーバの追加*ダイアログウィンドウにDNS名を入力して、*保存*をクリックします。

   入力したDNS名とサフィックス*Servers*で構成される新しいエントリが、ボックスに表示されます。UTMにより、指定したDNS名のDNSグループが自動的に作成され、新しいPOP3サーバエントリと関連付けられます。

2. **POP3サーバのプロパティを指定します。**
   *POP3サーバ*ボックスで、POP3サーバの前にある編集アイコンをクリックします。*サーバの編集*ダイアログウィンドウが開きます。次の設定を行います。

   名前：必要な場合は、POP3サーバの名前を変更します。

   ホスト：ボックスには、上で指定したDNS名のDNSグループが自動的に含まれています。追加ホストまたはDNSグループを追加または選択します。同じPOP3アカウントに対して機能するホストまたはDNSグループだけを追加していることを確認してください。定義を追加する方法は、*定義とユーザ > ネットワーク定義 > ネットワーク定義*ページで説明しています。

TLS証明書：ドロップダウンリストから証明書を選択します。この証明書は、TLS暗号化についてそれをサポートしているすべてのリモートホストとネゴシエートするために使用されます。証明書は、*サイト間VPN* > *証明書管理* > *証明書*タブで作成またはアップロードできます。

> 注 – TLS暗号化が機能するためには、*TLS設定*セクションの*TLS暗号化されたトラフィックだけをスキャン*チェックボックスを選択する必要があります。ここで指定していないか、TLS証明書を持たないPOP3サーバの場合、*TLS設定*セクションでデフォルトのTLS証明書を選択することができます。

コメント（オプション）：説明などの情報を追加します。

3. ***保存*をクリックします。**
   これで、POP3サーバが指定されます。

POP3サーバを指定しない場合にプロキシがメールを確認すると、プロキシは同じ接続でそのメールの代わりに、メールを隔離したことを受信者に通知するメッセージをただちに送ります。隔離されたメールは*メールマネージャ*で表示できますが、サーバやアカウントに関連付けられていないため、後から接続してリリースする（取り出して再配信する）ことはできません。一般的には、隔離されたメールのリリースは、プリフェッチされたメッセージのみで有効です。

以下の2つのシナリオがあります。

- POP3サーバを指定してプリフェッチを無効にした場合、プロキシは、隔離されたメールがどのサーバ/アカウントに属するかを追跡します。したがって、隔離されたEメールは、クライアントがメールボックスを次回ポーリングしたときにリリースできます。これが機能するには、プロキシは、どのIPアドレスがどのサーバに属するかを（お客様がメールクライアントで入力したFQDNによって）確実に特定する必要があります。
- POP3サーバを指定してプリフェッチを有効にした場合、POP3プロキシは新しいメッセージがないかどうかPOP3サーバを定期的に確認します。新しいメッセージが届いている場合、それはPOP3プロキシにコピーされ、スキャンされて、UTMのデータベースに保存されます。メッセージはPOP3サーバに留まります。クライアントは新しいメッセージをフェッチする（取り出す）とき、POP3プロキシと通信して、このデータベースからメッセージを取り出します。

プリフェッチをサポートしているPOP3プロキシには、以下のようなさまざまなメリットがあります。

- クライアントとプロキシ（またはその逆）のタイムアウトの問題はありません。
- メールを事前にスキャンするため、メッセージははるかに迅速に配信されます。
- ブロックされたメッセージはユーザポータルからリリースでき、次のフェッチに含まれます。

メッセージが悪意のコンテンツを含んでいたためにブロックされた場合、またはスパムと特定されたためにブロックされた場合は、クライアントには配信されません。それらのメッセージは隔離されます。隔離されたメッセージはユーザポータルの *メールマネージャ*セクションに保存され、そこで削除またはリリースされます。

プリフェッチモードを使用 : プリフェッチモードを有効にするには、このチェックボックスを選択して、1つ以上のPOP3サーバを*POP3サーバ*ボックスに追加します。

プリフェッチ間隔 : POP3プロキシがPOP3サーバに接触してメッセージをプリフェッチする時間間隔を選択します。

> 注 – メールクライアントがPOP3サーバへの接続を許可される間隔は、サーバごとに異なります。したがって、プリフェッチ間隔は、POP3サーバで許可されている間隔より短く設定しないようにしてください。この理由は、POP3サーバへのアクセスがブロックされると、POP3メッセージのダウンロードは失敗に終わるからです。
> また、複数のメールクライアントが同じPOP3アカウントをクエリする場合があることにも注意してください。POP3サーバからメッセージがフェッチされると、次回サーバにアクセスできるようになるまでタイマーが再始動します。このためにPOP3プロキシがPOP3サーバに4回連続してアクセスできないと(デフォルトでは15分ごとにアクセスを試行します)、アカウントのパスワードがプロキシのメールデータベースから削除され、メールクライアントがPOP3サーバにパスワードを再度送ってログインしない限り、メールはフェッチされなくなります。

隔離メールをサーバから削除 : このオプションを選択すると、隔離されたメッセージはPOP3サーバから即座に削除されます。これは、ユーザがUTM経由ではなく、たとえば、POP3サーバのWebポータル経由でPOP3サーバに接続した場合に、スパムやウイルスメッセージの受信を防ぐのに役立ちます。

メッセージを取り出した後にサーバからメッセージを削除するようにEメールクライアントが設定されている場合、この情報はデータベースにも保存されます。プロキシは、次回このPOP3アカウントのメッセージをプリフェッチするときに、サーバからそれらのメッセージを削除します。これは、クライアントがSophos UTMからメッセージをフェッチせず、かつ、削除コマンドが設定されていない限り、メッセージはPOP3サーバから削除されないことを意味します。したがって、たとえばEメールプロバイダーのWebポータルで依然読むことができます。
以下の場合、隔離されたメッセージはPOP3サーバから削除されます。

- メッセージをメールマネージャで手動で削除した場合。
- ユーザがユーザポータルでメッセージを手動で削除した場合。

- メッセージが(隔離レポートまたはユーザポータルのいずれかを介して)リリースされ、配信時にメッセージを削除するようにユーザのメールクライアントが設定されている場合。
- 通知メッセージが削除された場合。
- 保存期間が過ぎた場合(*メールマネージャ*の章の設定のセクションを参照してください)。

ただし、プリフェッチモードでは、隔離されたスパムメッセージは、クライアントコマンドではPOP3サーバから直接削除できません。

注 – プリフェッチ機能が正常に機能するためには、メールクライアントは少なくとも1回はPOP3サーバに接続する必要があります。これは、このユーザのためにPOP3メッセージをフェッチするには、Sophos UTMは、POP3サーバ名、ユーザ名、およびユーザのパスワードをデータベースに保存する必要があるからです。ただし、これは、Sophos「ユーザポータル」でPOP3アカウント資格情報を設定しても、アーカイブでき*ません*。プリフェッチされたメッセージをこのユーザのポータルと毎日の隔離レポートに表示するには、ユーザポータルでPOP3アカウント資格情報が必要です。

fetchmailユーザへの注記:セキュリティ上の理由から、メールサーバからのメールのダウンロードに`TOP`メソッドはサポートされていません。したがって、`TOP`によって受信したメッセージはスキャンできません。ただし、`fetchall`オプション(コマンドラインの`-a`)を指定するとスキャンできます。詳細は、fetchmailのマニュアルの「RETRまたはTOP」を参照してください。

優先文字コード

このセクションでは、メールヘッダは、何らかの理由でUTMによって変更された(例:BATV)メールヘッダで今後使用するUTF-8以外の文字コードを選択できます。この機能は、UTF-8を理解しないメールクライアントをユーザが使用している場合に便利です。一般に、メールヘッダのデフォルトの文字セットはすべての地域で問題なく機能します。したがって、この設定を変更するのは、これが絶対に必要であると確信している場合のみにしてください。不明な場合は、デフォルトの*UTF-8*にしておいてください。

TLS設定

TLS暗号化されたPOP3トラフィックのスキャン: 有効にすると、UTMはTLS暗号化されたPOP3トラフィックをスキャンします。これが機能するためには、POP3クライアントがアクセスするPOP3サーバに対してTLS証明書が指定されている必要があります(上記の*POP3サーバとプリフェッチ設定*のセクションおよび、下の*TLS証明書*チェックボックスを参照)。

無効にしていると、POP3クライアントがTLS経由でPOP3サーバにアクセスしようとしても、接続は確立されません。

TLS証明書：TLSをサポートし、上のPOP3サーバボックスでリストされていないか、適合するTLS証明書が関連付けられていないPOP3サーバにアクセスしようとするすべてのPOP3クライアントでの*TLS*暗号化で使用される証明書をドロップダウンリストから選択します。選択した証明書が、POP3クライアントに提示されます。通常は、POP3クライアントは、POP3サーバによって提示されたTLS証明書が、設定済みPOP3サーバの名前と一致していることを確認します。この理由から、大半のPOP3クライアントは証明書のホスト名が予想される設定済みPOP3サーバの名前と一致していないという警告を表示します。ただし、ユーザは警告を却下して、接続することができます。この警告を回避したい場合は、使用しているすべてのPOP3サーバを上記の*POP3サーバ*ボックスに追加し、それぞれについて一致するTLS証明書を設定します。

ここで証明書を選択していなければ、POP3クライアントが*POP3サーバ*ボックスでリストされていないか、適合するTLS証明書が関連付けられていないPOP3サーバにアクセスしようとしても、接続は確立されません。

ヒント – 証明書は、*サイト間 VPN* > *証明書管理* > *証明書*タブで作成またはアップロードできます。

10.4 暗号化

メールが個人的な目的やビジネス目的で使用する主な電子通信手段となって以来、プライバシーや認証に関する懸念が高まっています。メールは平文形式で伝送されますが、これを一般的に言うと、ハガキと同じようにすべての人が読めるということです。さらに、身元を偽るのが容易であるため、送信者が本当に本人であるかどうかを受信者が見分けられることは重要です。

通常、これらの問題はメールの暗号化とデジタル署名で解決できます。これにより、メールメッセージは電子的に署名され、暗号によって符号化されます。この結果、メールを開いてコンテンツを閲覧できるのはメッセージ受信者のみとなり（プライバシー）、送信者の身元が確認されるようになります（認証）。つまり、このプロセスでは「ハガキの電子版」を送付するという考えが否定され、書留郵便や配達証明郵便に近いプロセスとなります。

最先端の暗号技術では、対称と非対称という2種類のメール暗号化方式があります。いずれも標準的な方式となっており、さまざまなアプリケーションで利用されています。対称鍵暗号とは、送信者と受信者が同じ鍵を共有する暗号化方式です。

一方、非対称鍵暗号（あるいは公開鍵暗号）とは、各ユーザが2つの暗号鍵（データを暗号化する公開鍵と復号化のための秘密鍵（プライベート鍵））を持つ暗号方式です。公開鍵は自由に公開されますが、秘密鍵はユーザが厳重に保管します。

対称暗号方式の欠点として、送信者と受信者が安全に通信するためには、両者があらかじめ鍵を決め、これを互いだけの秘密として維持する必要があります。両者が離れた場所にいる場合、送信中に秘密鍵が開示されないようにしなければなりません。そのため、対称暗号方式では、鍵の受け渡しに関する問題が常に存在します。つまり、「他者に傍受されることなく受信者に鍵を伝えるにはどうすればいいか」という問題です。公開鍵暗号方式は、この問題に対処するために開発されました。公開鍵暗号方式では、ユーザは安全ではないチャネル上でも安全に通信することができ、あらかじめ共有鍵を決める必要はありません。

メール暗号化の必要性から、多種多様な公開鍵暗号化標準が生まれました。最も有名なのはS/MIMEとOpenPGPであり、Sophos UTMはその両方に対応しています。S/MIME(*Secure Multipurpose Internet Mail Extensions*)とは非対称暗号方式の標準であり、メール署名をMIMEにカプセル化します。通常、S/MIMEは公開鍵基盤(PKI)内で使用され、デジタル証明の階層構造に基づいており、信頼できるインスタンスとして認証局(CA)を必要とします。CAは、電子鍵のペアを身元情報とバインドして電子証明書を発行します。電子証明書は、パスポートなど従来からある身分証明書の電子版と考えることができます。技術的に言うと、CAは特定のX.500*識別名 DN*またはメールアドレスなどの*別名*に公開鍵をバインドして証明書を発行します。

デジタル証明書により、任意の鍵を使用する権利を主張する人にその権利があるかどうかを確認することができます。これは、ある人がCAを信頼しており、公開鍵がこのCAによって署名されていることを確認できるのであれば、この人はこの公開鍵が本当に所有者と主張する人のものであると安心できる、という考え方です。

一方、OpenPGP(*Pretty Good Privacy*)は、一般にWOT(*web of trust*)で採用されている非対称暗号方式を使用します。つまり、公開鍵は他のユーザによってデジタル署名され、署名するユーザは署名という行為によって、公開鍵とその人の関連性を保証します。

注 –S/MIMEとOpenPGPは類似のサービスを提供しますが、形式は大きく異なります。そのため、一方のプロトコルのユーザは、他方のプロトコルのユーザと通信できません。さらに、認証証明書を共有することもできません。

デフォルトでは、例えばS/MIME、OpenPGPおよびSPX暗号化が有効化されている場合、優先順位は、S/MIME、OpenPGP、そしてSPX暗号化の順になります。

メール暗号化は、ユーザに対して完全に透過的です。つまり、クライアント側で追加の暗号化ソフトウェアを用意する必要はありません。一般に暗号化では、送信先の証明書または公開鍵が手元にある必要があります。受信メッセージと送信メッセージに対し、メール暗号化機能は次のように機能します。

- デフォルトで、内部ユーザが送信したメッセージはスキャンされ、自動的に署名され、受信者の証明書(S/MIME)または公開鍵(OpenPGP)で暗号化されます(受信者のS/MIME証明

書またはOpenPGP公開鍵がUTM上にある場合)。

- UTMがS/MIME証明書またはOpenPGP公開鍵を認識している外部ユーザから送られてきた暗号化済み受信メッセージは、自動的に復号化され、悪質なコンテンツが含まれないかスキャンされます。メッセージの復号化のためには、内部ユーザのS/MIME鍵またはOpenPGP秘密鍵がUTMに存在している必要があります。

- UTMが認識できない外部ユーザから送られてきたか、セキュリティシステムが認識できない内部ユーザ向けの暗号化済み受信メッセージは、配達されるものの復号化はできません。従って、ウイルスやスパムのスキャンは行われません。個人用ファイアウォールなどでそのメールにマルウェアが含まれていないことを確認するのは、受信者(内部ユーザ)の責任となります。

- クライアント側ですでに暗号化されている送信メッセージは、受信者のS/MIME証明書またはOpenPGP公開鍵が不明な場合、受信者に直接送信されます。一方、受信者のS/MIME証明書またはOpenPGP公開鍵がわかる場合、メッセージは2回暗号化されます。あらかじめ暗号化されたメッセージに悪質なコンテンツが含まれないかスキャンすることはできません。

- 復号化が可能なのは受信メールのみです。ここで「受信」と見なされるためには、送信者のEメールアドレスのドメイン名がSMTPプロファイルの一部ではないことが条件です。たとえば、`jdoe@example.com`から送信されたメッセージを復号化するためには、`example.com`というドメインが*ルーティング*設定またはSMTPプロファイルのいずれにも設定されていないことが求められます。

- 署名/暗号化結果の概要は、各メールの件名行に記述されます。たとえば、あるメールが正しく署名され、S/MIMEで暗号化されると、「S/MIME:署名済み、暗号化済み(Signed and encrypted)」というテキストが件名の行に付加されます。

注 – メールクライアント(例: Microsoft Outlook または Mozilla Thunderbird)が署名済みまたは暗号化済みのメッセージにフッタを追加すると、署名が破壊されて無効になります。デジタル署名をクライアント側で作成する場合は、ウイルス対策チェックフッタオプションを無効にしてください。ただし、メール通信のプライバシーや認証を保ちながら、一般的なウイルス対策チェックフッタを使用する場合は、Sophos UTM の組み込みメール暗号化機能の使用を考慮してください。ゲートウェイ上でのメール暗号化では、デジタル署名を作成する前にフッタがメッセージに付加されるため、署名が損なわれることはありません。

10.4.1 グローバル

*Eメールプロテクション > 暗号化 > グローバル*タブでは、メール暗号化機能の基本設定を定義することができます。

注 – 暗号化はSMTPのみで機能し、POP3では機能しません。

メール暗号化を使用するためには、CA証明書とCA鍵から成る*認証局*（CA）を作成しておく必要があります。CA証明書はダウンロードしてローカルに保存することができます。さらに、図で示すように、他のユニットに外部CA（S/MIME認証局）としてインストールし、2つのSophos UTMユニット間で透過的なメール暗号化を実現することもできます。
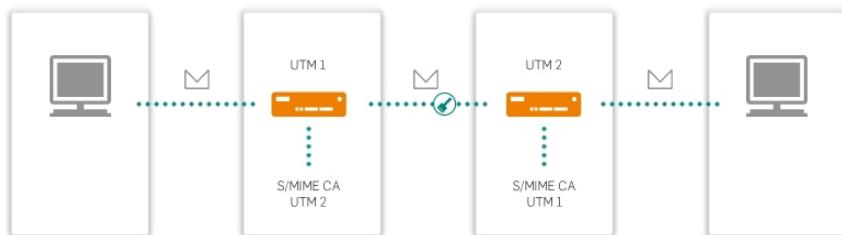
図 **19** メール暗号化：2つのSophos UTMユニットの使用

メール暗号化を設定するには、次の手順に従ってください。

1. **グローバルタブで、*メール暗号化*を有効化します。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、*メール暗号化認証局 CA* エリアが編集可能になります。

2. **認証局（CA）を作成します。**
   メール暗号化認証局 CA エリアのフォームに記入します。デフォルトで、このフォームには *マネジメント* > *システム設定* > *組織*タブの値が入力されています。

3. ***保存*をクリックします。**
   トグルスイッチが緑色になり、次の証明書と鍵が作成されます。

   - S/MIME CA証明書
   - OpenPGPポストマスタ鍵

   これが完了するまで数分かかる可能性があります。S/MIME CA証明書またはOpenPGPポストマスタ鍵のフィンガープリントが表示されない場合、WebAdminの右上隅にある*リロード*ボタンをクリックしてください。証明書と鍵は、ダウンロードしてローカルに保存できます。

*暗号化*メニューのすべての設定を工場出荷時のデフォルト設定にリセットするには、*メール暗号化 システムを今すぐリセット*ボタンを使用します。

10.4.2 オプション

*暗号化 > オプション*タブでは、Sophos UTMの公開鍵暗号フレームワーク内で使用されるデフォルトポリシを定義できます。

デフォルトポリシ: メールの暗号化に関するデフォルトポリシを指定します。これらの設定は、カスタマイズされた設定で上書きできます。

次の作業を実行できます。

- 送信メールに署名
- 外部宛送信メールの暗号化
- 内部宛受信メールの検証
- 受信メールの複合化

設定を保存するには*適用*をクリックします。

注 – 暗号化が機能するためには、送信者が*内部ユーザ*リストに含まれている必要があります。S/MIME証明書またはOpenPGP公開鍵がゲートウェイに存在する受信者に向けた送信メールは、デフォルトで暗号化されます。これらの受信者に対する暗号化を無効にするには、当該受信者のS/MIME証明書またはOpenPGP公開鍵を削除してください。証明書または公開鍵がUTMに不明の場合、メールは暗号化されずに送信されます。

S/MIME証明書の自動抽出

このオプションを選択すると、S/MIME証明書は受信メールから自動的に抽出されます。このとき、そのメールに添付された証明書が、信頼される認証局に署名されていることが条件となります。信頼される認証局とは、*Eメールプロテクション > 暗号化 > S/MIME認証局*タブに表示される、ユニットにあるCAです。さらに、証明書の自動抽出が機能するためには、Sophos UTMの時間と日付が、証明書の有効期間内である必要があります。証明書の抽出が成功すると、証明書は*Eメールプロテクション > 暗号化 > S/MIME証明書*タブに追加されます。これが完了するまで5～10分かかる可能性があります。設定を保存するには*適用*をクリックします。

OpenPGP鍵サーバ

OpenPGP鍵サーバは公開PGP鍵をホストします。ここで、OpenPGP鍵サーバを追加することができます。署名された受信メールや暗号化されるべき送信メールで、該当する公開鍵がUTMに不明の場合、UTMは所定のサーバから公開鍵を取得しようとします。

10.4.3 内部ユーザ

メッセージの署名と復号化を行うためには、S/MIME鍵またはOpenPGP秘密鍵がUTMに存在している必要があります。*暗号化* > *内部ユーザ*タブでは、メール暗号化を有効にするユーザに対して、個別のS/MIME鍵/証明書またはOpenPGP鍵ペア(あるいはその両方)を作成できます。

内部メールユーザを作成するには、次の手順に従います。

1. ***内部ユーザ*タブで*新規メール暗号化ユーザ*をクリックします。**
   *ユーザの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   メールアドレス:ユーザのメールアドレスを入力します。

   フルネーム:ユーザの名前を入力します。

   署名: 次の署名オプションを使用できます。

   - デフォルトポリシーを使用: *オプション*タブのポリシが使用されます。
   - オン:メールは、ユーザの証明書を使用して署名されます。
   - オフ:メールは署名されません。

   暗号化:次の暗号化オプションを使用できます。

   - デフォルトポリシーを使用: *オプション*タブのポリシが使用されます。
   - オン:メールは、受信者の公開鍵を使用して暗号化されます。
   - オフ:メールは暗号化されません。

   検証:次の検証オプションを使用できます。

   - デフォルトポリシーを使用: *オプション*タブのポリシが使用されます。
   - オン:メールは、送信者の公開鍵を使用して検証されます。
   - オフ:メールは検証されません。

   復号化:次の復号化オプションを使用できます。

   - デフォルトポリシーを使用: *オプション*タブのポリシが使用されます。
   - オン:メールは、ユーザの証明書を使用して復号化されます。
   - オフ:メールは復号化されません。

S/MIME: S/MIME証明書と鍵をシステムに自動生成させるか、証明書をPKCS#12形式でアップロードするかを選択します。証明書をアップロードする場合、PKCS#12ファイルの保護に使用されたパスフレーズを知っている必要があります。PKCS#12ファイルには、S/MIME鍵と証明書の両方が含まれていなければなりません。このPKCS#12ファイルに含まれているすべてのCA証明書は無視されます。

OpenPGP: 秘密鍵と公開鍵から成るOpenPGP鍵ペアをシステムに自動生成させるか、鍵ペアをASCII形式でアップロードするかを選択します。秘密鍵と公開鍵の両方が1つのファイルに格納されており、ファイルにパスフレーズが含まれていないことが必要です。

> 注 – あるユーザに対してS/MIMEとOpenPGPの両方が設定されている場合、このユーザから送信されるメールの署名はS/MIMEを使用して行われます。

コメント(オプション): 説明などの情報を追加します。

3. *保存*をクリックします。
新しいユーザが*内部ユーザ*リストに表示されます。

トグルスイッチを使用して、いずれかの鍵(または両方)の使用をオフにします。鍵を削除する必要はありません。

> 注 – ダウンロード用に提供されているファイルにはS/MIME証明書が含まれています。OpenPGP証明書により公開鍵が提供されます。セキュリティ上の理由から、OpenPGP秘密鍵およびS/MIME鍵をダウンロードすることはできません。

10.4.4 S/MIME認証局

*暗号化 > S/MIME認証局*タブで、メール暗号化のための認証局(CA)を管理できます。事前にインストールされているCAに加えて、外部認証局の証明書をアップロードすることもできます。ここでリストされ、有効化されているCAの1つによって署名されている証明書を持つすべての受信メールは、自動的に信頼されます。

> 注 – *Eメールプロテクション > 暗号化 > オプション*タブで*S/MIME証明書の自動抽出有効*オプションを選択した場合、ここにリストされ、有効化されたCAによって署名された証明書が自動的に抽出され、*Eメールプロテクション > 暗号化 > S/MIME証明書*タブに配置されます。

ローカルS/MIME認証局

信頼する外部認証局の証明書(例、公開鍵)をインポートすることができます。したがって、このCAによって署名された証明書を持つすべての受信メールも信頼されます。たとえば、他のSophos UTMユニットのCAをインストールすると、2つのSophos UTMユニット間でメールを透過的に暗号化することができます。

外部S/MIME認証局をインポートするには、次の手順に従います。

1. ***ローカルCAのアップロード*フィールドの横のフォルダアイコンをクリックします。**
   *ファイルのアップロード*ダイアログウィンドウが開きます。

2. **アップロードする証明書を選択します。**
   *参照*をクリックして、アップロードするCA証明書を選択します。次の証明書の拡張子がサポートされています。

   - `cer`、`crt`、`der`:これらの証明書タイプはバイナリで、基本的には同じです。
   - `pem`:Base64で暗号化されたDER証明書。

3. **証明書をアップロードします。**
   *アップロード開始*をクリックして、選択したCA証明書をアップロードします。

   証明書がインストールされ、*ローカルS/MIME認証局*エリアに表示されます。

ただし、CAが信頼できると考えられない場合、S/MIME認証局を無効にすることができます。S/MIME認証局の証明書を取り消すには、トグルスイッチをクリックします。トグルスイッチがグレーになり、SMTPプロキシはこのS/MIME認証局が署名したメールを受信しなくなります。証明書を削除するには、空白アイコンをクリックします。

ヒント – CA の指紋を表示するには、青色の情報アイコンをクリックしてください。

グローバルS/MIME認証局

ここに表示されるS/MIME CAのリストは、Mozilla Firefoxにあらかじめインストールされた S/MIME CAと同じです。これにより、これらのCAに基づいてPKIを管理しているコミュニケーションパートナーとお客様の間で、メールの暗号化が促進されます。ただし、CAが信頼できると考えられない場合、S/MIME認証局を無効にすることができます。S/MIME認証局の証明書を取り消すには、トグルスイッチをクリックします。トグルスイッチがグレーになり、SMTPプロキシはこのS/MIME認証局が署名したメールを受信しなくなります。

次のリンクは、有名なルート証明書のURLです。

- Trustcenter
- S-TRUST
- Thawte
- VeriSign
- GeoTrust

10.4.5 S/MIME証明書

*暗号化 > S/MIME証明書*タブでは、外部S/MIME証明書をインポートすることができます。証明書がここにリストされている受信者へのEメールは自動的に暗号化されます。特定の受信者に対する暗号化を無効にするには、リストから証明書を削除してください。

注 – 受信者に対して、OpenPGP公開鍵がS/MIME 証明書に追加的にインポートされると、メールはOpenPGPを使用して暗号化されます。

注 – S/MIME証明書を手動でアップロードすると、証明書に記載された人を識別できるCA証明書がなくても、証明書に関連付けられたメールアドレスからのメッセージが常に信頼されるようになります。つまり、S/MIME証明書を手動アップロードするということは、送信元に「信頼できる」というラベルを貼り付けるということになります。

外部S/MIME証明書をインポートするには、次の手順に従います。

1. ***S/MIME証明書*タブで*新規外部S/MIME証明書*をクリックします。**
   *S/MIME証明書の追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   形式: 証明書の形式を選択します。次の形式を選択できます。

   - `der`(バイナリ)
   - `pem`(ASCII)

   注 – Microsoft Windowsオペレーティングシステムでは、`der`形式と`pem`形式の両方に対してファイル拡張子`cer`を使用します。そのため、アップロードする証明書をバイナリ形式にするかASCII形式にするかを、あらかじめ決定しておく必要があります。次に、これに従ってドロップダウンリストで形式を選択します。

証明書:フォルダアイコンをクリックして、*ファイルのアップロード*ダイアログウィンドウを開きます。ファイルを選択し、*アップロード開始*をクリックします。

コメント(オプション):説明などの情報を追加します。

3. ***保存*をクリックします。**
新しいS/MIME証明書が*S/MIME証明書*リストに表示されます。

10.4.6 OpenPGP公開鍵

*暗号化 > OpenPGP公開鍵*タブでは、OpenPGP公開鍵をインストールすることができます。.asc形式のファイルを提供する必要があります。キーリング全体のアップロードがサポートされています。

> 注 – パスフレーズで保護されている鍵束ファイルはアップロードしないでください。

この鍵束ファイルに含まれるすべての公開鍵がインポートされ、メッセージの暗号化に使用できるようになります。公開鍵がここにリストされている受信者へのEメールは自動的に暗号化されます。特定の受信者に対する暗号化を無効にするには、リストから公開鍵を削除してください。

> 注 – 鍵ごとに1つのメールアドレスだけがサポートされます。1つの鍵に複数のアドレスが関連付けられている場合、「最初の」アドレスのみが使用されます(この順序は、OpenPGPでのアドレスのソート方法に応じています)。インポートしたい鍵に複数のアドレスが関連付けられている場合、その鍵をSophos UTMにインポートする前に、OpenPGPまたはその他のツールで不要なアドレスを削除する必要があります。

OpenPGP公開鍵をインポートするには、次の手順に従います。

1. ***OpenPGP公開鍵*タブで、*新規公開OpenPGP鍵 New Public OpenPGP Key(s)* をクリックします。**
*鍵束ファイルの追加*ダイアログボックスが開きます。

2. **OpenPGP鍵をアップロードします。**
フォルダアイコンをクリックして、*ファイルのアップロード*ダイアログウィンドウを開きます。ファイルを選択し、*アップロード開始*をクリックします。

鍵または鍵のリスト(ファイルに複数の鍵が含まれている場合)が表示されます。

3. **鍵を1つ以上選択し、*選択した鍵をインポート*をクリックします。**
鍵が*OpenPGP公開鍵*リストに表示されます。

> **注** – 鍵にはメールアドレスが1つ関連付けられていなければならず、関連付けられていない場合、インストールは失敗します。

10.5 SPX 暗号化

SPX（Secure PDF Exchange）暗号化は、メール暗号化の次世代バージョンです。クライアントレスであらゆる環境において非常に簡単に設定やカスタマイズを行うことができます。SPX 暗号化を使用を使用することにより、暗号化されていないメールメッセージや任意の添付がUTMへ送信される場合、パスワード付きの暗号化されたPDF文書に変換されます。UTMを受信者用パスワードを送信者が選択できるよう設定することができ、またサーバが受信者用パスワードを生成し、受信者がパスワードを保存できるようにする、もしくはサーバがワンタイムパスワードを生成するよう設定することが可能です。

SPX 暗号化が有効な場合におけるメールのSPX暗号化の2つの方法：

- 管理者はMicrosoft Outlookプラグインをダウンロードすることができます（*Eメールプロテクション > SPX 暗号化 > Sophos Outlook アドイン*の章を参照）。インストール後、Microsoft Outlookのユーザインターフェースに*暗号化*ボタンが表示されます。単一のメッセージを暗号化するには、ユーザが*暗号化*ボタンを有効にする必要があり、次にメッセージを書いて送信します。送信者が有効なパスワードを入力していないなどの手違いが発生した際、設定されている場合には通知が送信されます。

  > **注** – Outlookを使用していない場合、ヘッダフィールドのX-Sophos-SPX-Encryptで*はい*と設定することにより、SPX暗号化をトリガすることもできます。

- Data Protection機能では、機密データを含むメールを自動的にSPX 暗号化するよう指定することができます（*SMTP > データ保護*タブを参照）。

その後、暗号化されたメッセージが受信者のメールサーバへ送信されます。Adobe Readerを使用することにより、受信者はPDFの暗号化に使用されたパスワードを使用し、メッセージを復号化することができます。SPXで暗号化されたメールメッセージは、「ネイティブ」またはサードパーティのPDFファイルサポートを持つBlackberryやWindows Mobileデバイスを含む、一般向けのすべてのスマートフォンでアクセス可能です。

SPX 返信ポータルを使用することにより、受信者画安全な方法でメールに返信することが可能です。安全な返信や未使用パスワードに対し有効期間を設定することが可能です（*Eメールプロテクション > SPX 暗号化 > SPX 設定*の章を参照）。

SPX暗号化はSMTP設定モード、シンプルモード、プロファイルモードで有効にすることができます。シンプルモードを使用している場合、グローバルSPXテンプレートが選択されます。SPXテンプレートがPDFファイル、パスワード設定、受信者の手順、およびSPX返信ポータル設定を定義します。プロファイルモードを使用している場合、別のSMTPプロファイルに対し、別のSPXテンプレートを定義することができます。そのため、さまざまな顧客のドメインを管理している場合、別の会社ロゴや文章を含むカスタマイズされたSPXテンプレートを割り当てることができます。

10.5.1 SPX設定

*SPX暗号化 > SPX設定*タブで、SPX暗号化を有効にし、すべてのSMTPユーザに対する一般設定を行います。

SPX暗号化を設定するには、次の手順に従ってください。

1. **SPX暗号化を有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチが緑色に変わります。

2. このタブのセクションで、必要なグローバル設定を行います。

3. *SPXテンプレート*タブで、既存の**Sophos**デフォルトテンプレートを変更および/または新規**SPX**テンプレートを追加します。

4. ***SMTP** > グローバル*タブで、グローバル**SPX**テンプレートを選択します。

5. **SMTP**をプロファイルモードで使用している場合、オプションで、各**SMTP**プロファイルに対し、希望の**SPX**テンプレートを選択します。

> 注 – ユーザにMicrosoft Outlookプラグイン経由でメールメッセージのSPX暗号化を行ってほしい場合、ユーザに*Eメールプロテクション > SPX暗号化 > Sophos Outlookアドイン*タブへのアクセスがあることを確認してください。別のメールメッセンジャを使用している場合、自分で手動によりヘッダを設定しなければなりません。

SPX暗号化優先

SPX暗号を優先:これを有効にしS/MIMEおよび/またはOpenPGPが有効化されている場合、SPX暗号がS/MIMEやOpenPGPより優先されます。

SPXパスワード設定

最小長:送信者によって指定されたパスワードに対する文字の最小数。

必須特殊文字：有効にすると、送信者によって指定されたパスワードに最低1つの特殊文字が含まれていなければなりません(非英数字および空白類文字は特殊文字として扱われる)。

設定を保存するには*適用*をクリックします。

SPXパスワードリセット

パスワードのリセット：ここで受信者のパスワードを削除することができます。受信者のメールアドレスを入力し、*適用*をクリックします。

SPXポータル設定

SPX返信ポータルを有効化：SPX返信ポータルを提供するインターフェースを選択します。このWebインターフェースにより、SPX暗号化メッセージの受信者が送信者に対し、安全に返信することができるようになります。多数の設定により、これを外部インタフェースにします。

ポート：SPX返信ポータルがリスンするポートを入力します。

設定を保存するには*適用*をクリックします。

SPXポータルおよびパスワードの有効期間の設定

安全な返信を許可：SPX暗号化メッセージの受信者に対し、SPX返信ポータル経由で返信が可能な期間を指定します。

未使用パスワードの保持：パスワードが使用されない場合の有効期間を指定します。

例えば*未使用パスワードの保持*が3日に設定されている場合において、SPX暗号化メッセージが指定の受信者に送信されなかった場合、パスワードは0時に期限切れとなります。

> **注** – *未使用パスワードの保持*が0日に設定されている場合、パスワードは保存され、0時に期限切れとなります。

設定を保存するには*適用*をクリックします。

SPX通知設定

エラーについての通知を送信：SPXエラーが発生した場合、だれに通知を送信するか指定します。管理者、送信者、双方に送信する、またはまったく通知を送信しないことができます。エラーメッセージは、常時、SMTPログにリストされます。

> ヒント – SPXエラーメッセージは、*管理* > *カスタマイズ* > *メール メッセージ*タブでカスタマイズできます。

設定を保存するには*適用*をクリックします。

10.5.2 SPXテンプレート

SPX暗号化 > *SPXテンプレート*タブで、既存のデフォルトSophosテンプレートを変更し、新規SPXテンプレートを定義することができます。SMTPをシンプルモードで使用している場合、*SMTP* > *グローバル*タブですべてのSMTPユーザに対し、グローバルSPXテンプレートを選択することができます。SMTPをプロファイルモードで使用している場合、*SMTPプロファイル*タブで別のSPXテンプレートから別のSMTPプロファイルに割り当てることができます。

SPX暗号化を設定するには、次の手順に従ってください。

1. ***新規SPXテンプレート*をクリックします。**
   *SPXテンプレートの追加*ダイアログボックスが開きます。

   > ヒント – Sophosデフォルトテンプレートには、便利な設定や文例などが含まれています。そのため、最初から新規テンプレートを作成する代わりに*複製*ボタンを使用し、既存のテンプレートを複製することも考慮に入れます。

   > 注 –通知送信者は、*管理* > *通知送信者*で設定されるメールアドレスです。

2. **次の設定を行います。**
   テンプレート名：テンプレートを説明する名前を入力します。

3. **次の基本設定を行います。**
   コメント(オプション)：説明などの情報を追加します。

   組織名：設定によりますが、組織名は、管理者やメール送信者に送信されるSPX関連の通知に表示されます。

   PDF カバーページ：追加の最初のページに暗号化されたPDFファイルを希望する際に選択します。デフォルトページまたはカスタムページを使用できます。カスタムページを使用する場合、フォルダーアイコンを通して1ページのPDFファイルをアップロードします。

   PDF暗号化：PDFファイルの暗号化モードを選択します。一部のPDFビューアーでは、AES/256暗号化されたPDFファイルを読むことができませんのでご注意ください。

   ラベル言語：受信者に転送されるメールのラベルの表示言語を選択します。メールには、例として*フォーム*、*宛先*、*送信者*または*件名*などのフィールドが含まれます。

   ページサイズ：PDFファイルのページサイズを選択します。

Sophosロゴを削除：デフォルトのSophosロゴと指定された会社ロゴを置き換える場合に、*管理* > *カスタマイズ* > *一般*タブでこのオプションを有効にします。ロゴが表示される2ヶ所：受信者に送信される暗号化メールのフッタおよび、PDFファイルの*返信*ボタンを通じて生成された返信メッセージのフッタ。

4. **次のパスワード設定を行います。**
パスワードタイプ：暗号化されたメールメッセージへのアクセスに対するパスワードの生成方法を選択します。*受信者が設定*する場合を除き、送信者は選択したタイプに合せて、受信者宛てのパスワード転送を安全な方法で行うことを常に心がけます。

- すべてのメールに対する生成されたワンタイムパスワード：影響する各メールに対し、UTMは自動的に新規パスワードを作成します。このパスワードは送信者に送信されます。

- 受信者に対する生成および保存：初めてのメールが受信者に送信される際、UTMは自動的に受信者指定パスワードを作成します。このパスワードは送信者に送信されます。次のメールから、自動的に同じパスワードが使用されます。一定の期間パスワードが使用されない場合、期限切れとなりますが、管理者によってリセットが可能です。*SPX設定*タブを参照してください。

- 送信者による指定：メール送信者が自分でパスワードを入力する場合に選択します。この場合、送信者は次のフォーマットを使用し、*件名*フィールドにパスワードを記入する必要があります。`<password>`の `[secure:<password>]<subject text>` が暗号化されたPDF ファイルを開くためのパスワード、`<subject text>` がランダムの件名を開くパスワードです。当然のことながら、パスワードは受信者にメールが送信される前に、UTMによって削除されます。

  注 – このオプションを使用したテンプレートは、Data Protectionと組み合わせて使用することはできません。Data Protectionでは、送信者はメールが暗号化されていることを事前に知らないため、*件名*フィールドにパスワードを入力しません。UTMが指定のパスワードなしでメールのSPX暗号化を行おうとする場合、送信者はパスワードが不明との情報が記載されたエラーメッセージを受信します。

- 受信者が設定：メール受信者が自分でパスワードを入力する場合に選択します。この場合受信者は、パスワードを登録できるUTMポータルに繋がるリンクを受け取ります。登録後に受信者は、現在の暗号化メールを見ることができるようになります。また同じパスワードを利用して、この送信者または同組織の別の送信者からの、将来の暗号化メールも見ることができます。

> 注 – 受信者がパスワードを入力しなかった場合、メールは*Eメールプロテクション*> *メールマネージャ*> *グローバル*タブに表示されます。

通知の件名（*送信者による指定*オプションなし）：UTMからメール送信者に送信されるメールの件名にパスワードが含まれています。ここで受信者名に対し%%ENVELOPE_TO%%などの変数を使用することができます。

通知の本文（*送信者による指定*オプションなし）：UTMからメール送信者に送信されるメールの本文にパスワードが含まれています。ここでパスワードに対し%%GENERATED_PASSWORD%%などの変数を使用することができます。

> ヒント – このタブのSophosデフォルトSPXテンプレートには、使用可能なすべての変数が含まれ、役立つ通知の例が挙げられています。

5. **次の受信者の手順の設定を行います。**
受信者用手順：UTMからメール受信者に送信されるメールの本文に暗号化されたメールに関する手順が含まれています。シンプルなHTMLマークアップとハイパーリンクを使用できます。また%%ORGANIZATION_NAME%%などの変数を使用することもできます。

> ヒント – このタブのSophosデフォルトSPXテンプレートには、使用可能なすべての変数が含まれ、役立つ受信者用手順の例が挙げられています。

ヘッダ画像/フッタ画像：UTMからメール受信者へのメールにヘッダ画像/フッタ画像を含める場合に選択します。適切な文章付きのオレンジ色のエンベロープのデフォルト画像、またはカスタム画像を使用することができます。カスタム画像を使用する場合、フォルダーアイコンを通してJPG、GIF、またはPNGファイルをアップロードします。推奨サイズは752 x 69ピクセルです。

6. **次のSPXポータル設定を行います。**
SPX返信ポータルを有効化：有効にすると、受信者に送信される暗号化されたPDFファイルに*返信*ボタンが含まれます。このボタンを使用し、受信者は送信者に暗号化されたメール返信を送信するためのSPX返信ポータルにアクセスすることができます。

返信に原文を含める：有効にすると、受信者からの返信に元のメールの文章が自動的に含まれます。

ポータルヘッダ画像/ポータルフッタ画像：SPX返信ポータルにヘッダ画像および/またはフッタ画像を含める場合に選択します。適切な文章付きのオレンジ色のエンベロープのデフォ

ルト画像、またはカスタム画像を使用することができます。カスタム画像を使用する場合、フォルダーアイコンを通してJPG、GIF、またはPNGファイルをアップロードします。推奨サイズは752 x 69ピクセルです。

7. *保存*をクリックします。
*SPXテンプレート*リストにSPXテンプレートが作成され、表示されます。

SPXテンプレートを編集または削除するには、対応するボタンをクリックします。

10.5.3 Sophos Outlookアドイン

*Eメールプロテクション > SPX暗号化 > Sophos Outlookアドイン*タブで、SophosWebサイトをナビゲートすることができ、MySophos資格情報を使用しSophosOutlookアドインをダウンロードすることも可能です。

Outlookアドインは、組織から発信される機密情報を含むメッセージの暗号化を簡素化します。ダウンロードおよびドキュメンテーションのインストールについては、SophosWebサイトを参照してください。

パラメータを使用してインストーラを実行 : msiexec /qr /i SophosOutlookAddInSetup.msi T=1 EC=3 C=1 I=1

10.6 隔離レポート

Sophos UTM は、さまざまな理由からブロックされて隔離場所にリダイレクトされたすべてのメッセージ (SMTP および POP3)を含むメールの隔離場所を用意しています。ここには、配信待ちのメッセージ、悪意あるソフトウェアに感染したメッセージ、疑わしい添付ファイルを含むメッセージ、スパムと特定されたもの、または単に不要な表現を含むメッセージが含まれます。

メッセージが間違って隔離されて保留されるリスク(いわゆる*誤検出*)を最小限に抑えるために、Sophos UTMは、隔離されたメッセージについて報告する隔離レポートをユーザに毎日送信します。ユーザーに複数のメールアドレスが設定されている場合は、それぞれのメールアドレスに個々の隔離レポートが送信されます。ユーザーポータルで追加の POP3 アカウントが設定されており、Sophos UTM の POP3 プロキシが*プリフェッチ*モード (POP3 サーバーからメッセージをプリフェッチし、ローカルデータベースに保存することが可能) である場合にも、これは適用されます。隔離レポートでは、ユーザはスパムエントリをクリックしてメッセージを隔離場所からリリースしたり、今後のために送信者をホワイトリストに追加できます。

隔離レポートの詳細について、以下に少し説明します。

- 隔離レポートは、メールアドレスがSMTPプロファイルに含まれているドメインの一部であるユーザに対してのみ送信されます。隔離レポートには、*SMTP* > *ルーティング*タブの *ドメイン* ボックスで指定したものや、SMTPプロファイルの *ドメイン*ボックスで指定したものが含まれます。

- POP3 *プリフェッチ*オプションが無効の場合、このアカウントに送信された隔離されたメッセージは隔離レポートには表示されません。代わりに、各ユーザーの受信トレイに、一般的な Sophos POP3 のブロックメッセージが表示されます。したがって、隔離レポートまたはユーザポータルを使用してメッセージをリリースすることはできません。このようなメールは、管理者が zip 形式で*メールマネージャ*からダウンロードすることでのみ配信できます。

- *詳細*タブで、管理者は、ユーザーがリリースできる隔離メールのタイプを定義します。デフォルトでは、隔離場所からリリースできるのは、スパムメールだけです。他の理由で隔離されたメッセージ(ウイルスや疑わしい添付ファイルを含むメッセージなど)は、Sophos UTMのメールマネージャで管理者によってのみ隔離場所からリリースできます。さらに、ユーザーは、現在隔離されているすべてのメッセージをSophosユーザーポータルで確認することができます。

- スパムメールに複数の受信者がいる場合は、メーリングリストの場合と同様に、受信者の誰かがそのメールをリリースすると、メーリングリストのメールアドレスがシステムで設定されている場合は、そのメールはその受信者のみにリリースされます。そうでない場合は、そのメールはすべての受信者に同時に配信されます。詳細は、*Eメールプロテクション* > *隔離レポート* > *除外*タブの*内部メーリングリストの定義*オプションを参照してください。

- 管理者は、Sophos UTMでユーザーが設定されていない SMTP メールアドレスに送信されたメールを、隔離レポートまたはメールマネージャからリリースできます(ホワイトリストへの追加はしない)。ただし、このユーザが設定されていないため、ユーザポータルへのアクセスはできません。

- メーリングリストに送信されたスパムメールはホワイトリストに追加できません。

- メールクライアントでメールのヘッダを正しくエンコードしないとデイリーの隔離レポートのメールが正しく表示されない場合があります。

10.6.1 グローバル

隔離レポート > *グローバル*タブで、デイリーの隔離レポートの送信時刻を定義して、隔離レポートに表示されるメッセージテキストを記述できます。

隔離レポートの設定を編集するには、隔離レポートを有効にします。トグルスイッチをクリックします。
トグルスイッチが緑色に変わります。

レポート送信時刻

ここでデイリーの隔離レポートの送信時刻を定義できます。ドロップダウンリストで時刻を選択し、*適用*をクリックします。

追加のレポートを送信することもできます。これを行うには、*追加のレポートを送信*チェックボックスにチェックを入れ、時刻を設定して、*適用*をクリックします。

カスタマイズ可能なメッセージテキスト

ここで、隔離レポートの序文となるテキストをカスタマイズできます。必要に応じてメッセージテキストを変更して、*適用*をクリックします。

> 注 – カスタマイズ可能なメッセージテキストボックスではHTMLタグは使用できません。

> 注 – ホームユーザライセンスを使用している場合は、カスタマイズできません。

> 注 – 通知送信者は、*マネジメント* > *通知* > *グローバル*タブで設定されるメールアドレスです。

10.6.2 除外

隔離レポート > *除外*タブで、デイリーの隔離レポートの受信から除外するEメールアドレスのスキップリストを定義できます。

隔離レポートのスキップ

ここで隔離通知を送信しない内部メールアドレスを設定できます。ここにメールアドレスがリストされているユーザは、デイリーの隔離レポートを受信しません。完全なメールアドレスを入力するか、または`*@example.com`のようにアスタリスク(*)をワイルドカードとして使用できます。

> 注 – スキップリストはSMTP隔離レポートにのみ適用されます。それぞれのユーザに指定されたPOP3アカウントがある場合は、POP3隔離レポートはそれにもかかわらず送信されます。

内部メーリングリストの定義

メーリングリストのメールアドレスが*メーリングリストアドレスパターン*ボックスで設定されている場合に(例:`newsletter@example.com`)、このメーリングリストに送信されたスパムメッセージが検知されてメールの隔離場所にリダイレクトされたときは、このメーリングリストに含まれるすべての受信者の隔離レポートがこのスパムメッセージへのリンクを含みます。したがって、各受信者は、受

信者が隔離レポートの *リリース*リンクをクリックすると表示されるユーザプロンプトに自身のメールアドレスを入力することで、このスパムメッセージを個々にリリースできます。

注 – メーリングリストは隔離レポートまたはユーザポータルでホワイトリスト化できません。

代わりに、特定メーリングリストのメールアドレスを、追加Eメールアドレスとしてローカルユーザのプロファイルに入力することで、このユーザを一種のメールマネージャに設定できます。すると、このユーザの隔離レポートのみがメーリングリストに送信されたスパムメッセージへのリンクを含むようになります。*リリース*リンクをクリックすると、そのメーリングリストのすべての受信者に一度にスパムメッセージが送信されます。

注 – メーリングリストのメールアドレスがユーザのプロファイルの追加メールアドレスとして設定されている場合は、そのメーリングリストに送信されたスパムメッセージへのリンクは、そのメーリングリストの受信者には表示されません。

ただし、メーリングリストのメールアドレスがユーザのプロファイルおよび *メーリングリストアドレスパターン*ボックスの両方で追加メールアドレスとして設定されている場合は、そのユーザの隔離レポートの *リリース*リンクからユーザプロンプトが開きます。そこでスパムメッセージの転送先のそれぞれのEメールアドレスを手動で入力して、スパムメールの受信者を決定できます。

最後に、メーリングリストのメールアドレスがユーザプロファイルとメーリングリストアドレスパターンのどちらでも追加メールアドレスとして設定されていない場合は、メーリングリストに送信されたスパムメッセージは通常のメールのように扱われます。つまり、受信者の誰かがスパムメールをリリースすると、それはメーリングリストのすべての受信者に送信されます。

要約すると、メーリングリストのメールアドレスをメーリングリストアドレスパターンとして設定すると、隔離レポートにスパムメッセージへのリンクを持つ各ユーザは、スパムメッセージのリリース先のメールアドレスを入力するように要求されることになります。

10.6.3 詳細

隔離レポート > *詳細*タブで、デイリーの隔離レポートに含まれる *リリース*リンクに代替ホスト名とポート番号を設定できます。また、スパムメールのリリースオプションを変更することもできます。

隔離レポート詳細オプション

ホスト名：デフォルトでは、*マネジメント* > *システム設定* > *ホスト名*タブのゲートウェイのホスト名です。ゲートウェイが送信する隔離レポートには、ハイパーリンクなどが含まれており、ユーザはこれをクリックしてメール隔離場所からメッセージをリリースできます。デフォルトでは、これらのリンク

はここで指定したホスト名をポイントしています。ユーザがインターネット上でメールをリリースできるようにしたい場合は、パブリックに解決できる代替ホスト名をここに入力する必要があります。

ポート: デフォルトでは、ポート`3840`が設定されています。ポートは、`1024`〜`65535`の範囲内でどの値にでも変更できます。

許可ネットワーク: メールリリースサービスへの接続を許可するネットワークも指定できます。デフォルトでは、内部ネットワークのみが選択されています。

設定を保存するには*適用*をクリックします。

リリースオプション

ここで、ユーザがリリース可能な隔離メッセージのタイプを選択できます。以下のオプションから選択できます。

- マルウェア
- スパム
- 表現フィルタ
- ファイル拡張子
- スキャン不可
- MIMEタイプ
- その他

設定を保存するには*適用*をクリックします。

10.7 メールマネージャ

メールマネージャとは、機器に現在保存されているすべてのメールメッセージを管理および整理するための管理ツールです。配信待ちのメッセージや、悪意あるソフトウェアに感染している隔離メッセージ、疑わしい添付ファイルが添付されている隔離メッセージ、スパムとして識別された隔離メッセージ、または好ましくない表現が含まれている隔離メッセージなどが表示されます。メッセージをダウンロード、リリース、削除する前に、メールマネージャを使用してすべてのメッセージをレビューすることができます。メールマネージャは UTF-8 に完全に対応しています。

10.7.1 メールマネージャウィンドウ

SMTP Quarantine | SMTP Spool | SMTP Log | POP3 Quarantine | Close |

Result Filter: Delivered Rejected Quarantined Blackholed Cancelled Bounced Deleted Unknown

Reason Filter: Malware Spam Expression File Extension MIME Type Unscannable Other RDNS/HELO RBL Host Blacklist Sender Blacklist BATV Rcpt verification SPF

Profile/Domain: All　IP/Net/Address/Subj. substring:　Received date: until

Page 1 of 1　10 events match the filter settings. Sort by event time, newest first , and show 20 entries per page.

Date	IP / Size	Time	Sender / Subject	Recipient	Result
2012-08-23 14:00	10.8.1.161 2kB		sender@domain.local bad attachment	testuser28@vinet.qa	Rejected: Malware (EICAR-AV-Test)
2012-08-23 14:00	10.8.1.161 1kB	2 s	sender@domain.local bad attachment	testuser28@vinet.qa	Quarantined: Malware (Eicar-Test-Signature)
2012-08-23 13:59	10.8.1.161 1kB	9 s	sender@domain.local bad attachment	testuser28@vinet.qa	Quarantined: Malware (Eicar-Test-Signature)
2012-08-23 13:57	10.8.1.161 1kB	3 s	sender@domain.local simple mail 3	testuser28@vinet.qa	Quarantined: Spam
2012-08-23 13:56	10.8.1.161 1kB	6 s	sender@domain.local RPD Spam test: Spam	testuser28@vinet.qa	Blackholed: Spam (confirmed)
2012-08-23 13:56	10.8.1.161 1kB		sender@domain.local RPD Spam test: Spam	testuser28@vinet.qa	Rejected: Spam (confirmed)
2012-08-23 13:55	10.8.1.161 1kB	5 s	sender@domain.local RPD Spam test: Bulk	testuser28@vinet.qa	Quarantined: Spam
2012-08-23 13:54	10.8.1.161 1kB	2 s	sender@domain.local simple mail 2	testuser28@vinet.qa	Delivered -> 10.0.3.13 (vlinux3.vinet.qa)
2012-08-23 13:53	10.8.1.161 1kB	11 s	sender@domain.local simple mail	testuser28@vinet.qa	Delivered -> 10.0.3.13 (vlinux3.vinet.qa)
2012-08-23 13:53	10.8.1.161 1kB		sender@domain.local	testuser28@vinet.qa	Rejected: RDNS/HELO (RDNS missing)

図**20** のメールマネージャSophos UTM

メールマネージャウィンドウを開くには、*Eメールプロテクション > メールマネージャ > グローバル*タブの*新しいウィンドウでメールマネージャを開く*ボタンをクリックします。メールマネージャは、次の5つのタブに分割されています。

- **SMTP Quarantine**:現在隔離されているすべてのメッセージを表示します。
- **SMTP Spool**:現在`/var/spool`にあるすべてのメッセージを表示します。これらのメッセージは、配信待ちであるか、エラーが発生したためにスプールに含まれている可能性があります。
- **SMTP Log**:SMTP経由で処理されたすべてのメッセージの配信ログを表示します。
- **POP3 Quarantine**:POP3経由でフェッチされた現在隔離されているすべてのメッセージを表示します。
- 閉じる:これをクリックすると、メールマネージャウィンドウが閉じます。

10.7.1.1 SMTP/POP3隔離

SMTPおよびPOP3隔離内のメッセージは、それぞれの隔離理由別に表示することができます。

- マルウェア
- スパム
- 表現フィルタ
- ファイル拡張子
- MIMEタイプ（SMTPのみ）
- スキャン不可
- その他

チェックボックスを使用して、隔離理由を選択/選択解除します。隔離理由のチェックボックスをダブルクリックすると、この理由だけが選択されます。

ヒント – メッセージを表示するには、メッセージをダブルクリックします。

Profile/Domain プロファイル/ドメイン ：プロファイル/ドメインを選択すると、そのプロファイル/ドメインのメッセージのみが表示されます。

Sender/Rcpt/Subject substring 送信者/受信者/件名サブストリング ：ここでは、メッセージ内で検索する送信者、受信者、または件名を入力します。

Received date 受信日 ：特定の期間内に処理されたメッセージのみを表示するには、日付を入力するか、カレンダアイコンで日付を選択します。

Sort by ソート順 ：デフォルトでは、受信時刻によりリストがソートされています。ここでは、別のソート基準を選択できます。

and show 表示 ：チェックボックスで、ページ当たり20、50、100、250、500、1000、またはすべてのメッセージを表示できます。すべてのメッセージの表示には時間がかかる場合があります。

各メッセージの前にあるチェックボックスを使用するか、メッセージをクリックして、選択したメッセージにアクションを適用します。次の作業を実行できます。

- 表示（個別のメッセージでのみ使用可能）：メールのコンテンツを示すウィンドウを開きます。
- **Download** ダウンロード ：選択されたメッセージをダウンロードします。
- **Delete** 削除 ：選択されたメッセージを削除します。これを取り消すことはできません。
- **Release** リリース ：選択されたメッセージを隔離からリリースします。
- **Release and report as false positive** リリースし、誤検出として報告 ：選択したメッセージを隔離からリリースし、スパムスキャンエンジンに誤検出として報告します。

隔離に保留されているメッセージをすべてリリースできるのは管理者だけです。Sophosユーザポータルでメッセージを確認したユーザは、明示的に許可されているメッセージのみをリリースすることができます。この権限付与設定は、*Eメールプロテクション* > *隔離レポート* > *詳細*タブで確認できます。

Select global cleanup action グローバルクリーンアップアクションの選択 :ここには、メッセージに対してグローバルに適用されるさまざまな削除オプションがあります。つまり、選択されていないメッセージや表示されていないメッセージにもオプションが適用されます。

警告 – メッセージの削除を取り消すことはできません。

10.7.1.2 SMTP Spool

ここには、配信待ちメッセージまたはエラーが発生したメッセージが表示されます。配信ログは、メッセージヘッダの一部でもあります。次のチェックボックスを使用して、表示するメッセージのタイプを1つだけ選択してください。

- **Waiting** 待機中 :配信待ちのメッセージ。
- **Error** エラー :エラーが発生したメッセージ。あるメッセージでエラーが複数回発生した場合は、SophosパートナーまたはSophosサポートチームに報告してください。

ヒント – メッセージを表示するには、メッセージをダブルクリックします。

Profile/Domain プロファイル/ドメイン :プロファイル/ドメインを選択すると、そのプロファイル/ドメインのメッセージのみが表示されます。

Sender/Rcpt/Subject substring 送信者/受信者/件名サブストリング :ここでは、メッセージ内で検索する送信者、受信者、または件名を入力します。

Received date 受信日 :特定の期間内に処理されたメッセージのみを表示するには、日付を入力するか、カレンダアイコンで日付を選択します。

Sort by ソート順 :デフォルトでは、受信時刻によりリストがソートされています。ここでは、別のソート基準を選択できます。

and show 表示 :チェックボックスで、ページ当たり20、50、100、250、500、1000、またはすべてのメッセージを表示できます。すべてのメッセージの表示には時間がかかる場合があります。

各メッセージの前にあるチェックボックスを使用するか、メッセージをクリックして、選択したメッセージにアクションを適用します。次の作業を実行できます。

- **Download** ダウンロード :選択されたメッセージをダウンロードします。
- **Retry** 再試行 :選択されたメッセージの配信を即時に再試行します。
- **Delete** 削除 :選択されたメッセージを削除します。これを取り消すことはできません。
- **Bounce** バウンス :選択されたメッセージをバウンスします。送信者には、メッセージの配信がキャンセルされたことを伝えるメッセージが送信されます。

グローバルクリーンアップアクションの選択:ここには、メッセージに対してグローバルに適用される再試行オプションとさまざまな削除オプションがあります。つまり、選択されていないメッセージや表示されていないメッセージにもオプションが適用されます。

警告 – メッセージの削除を取り消すことはできません。

10.7.1.3 SMTP Log

*SMTP Log*には、SMTP経由で処理されたすべてのメッセージのログメッセージが表示されます。

Result Filter 結果フィルタ :表示されるメッセージのタイプを選択するには、該当するチェックボックスにチェックを入れます。

- **Delivered** 配信済み :配信が成功したメッセージ。
- **Rejected** リジェクト :UTMに拒否されたメッセージ。
- **Quarantined** 隔離 :隔離されたメッセージ。
- **Blackholed** ブラックホール; 削除済み :通知なしで削除されたメッセージ。
- **Canceled** キャンセル :*SMTPスプール*に手動でバウンスされたメッセージ。
- **Bounced** バウンス :ルーティング設定が正しくないなどの理由により、配信できないメッセージ。
- **Deleted** 削除済み :手動で削除されたメッセージ。
- **Unknown** 不明 :ステータスが不明なメッセージ。

Result Filter 結果フィルタ アイテムの選択/選択解除を切り替えるには、チェックボックスを使用します。アイテムをダブルクリックすると、そのアイテムだけが選択されます。

Reason Filter 理由フィルタ :メッセージログの表示をさらにフィルタするには、チェックボックスを使用します。

ヒント – メッセージログを表示するには、メッセージログをダブルクリックします。IPアドレスを解決するには、メッセージのサーバアイコンをクリックします。アスタリスク(*)は、リバースDNSルックアップが成功したことを示します。

Profile/Domain *プロファイル/ドメイン*:プロファイル/ドメインを選択すると、そのプロファイル/ドメインのメッセージのみが表示されます。

IP/Net/Address/Subj. substring **IP/***ネット/アドレス/件名 サブストリング*:ここでは、SMTPログメッセージ内で検索するIPアドレス、ネットワークアドレス、または件名を入力します。

Received date *受信日*:特定の期間内に処理されたメッセージのみを表示するには、日付を入力するか、カレンダアイコンで日付を選択します。

Sort by(*ソート基準***)**:デフォルトでは、イベント時刻によりリストがソートされています。メッセージは、イベント時間、送信者アドレス、メッセージサイズを基準にソートできます。

and show *表示*:チェックボックスで、ページ当たり20、50、100、250、500、1000、またはすべてのメッセージを表示できます。すべてのメッセージの表示には時間がかかる場合があります。

10.7.2 グローバル

メールマネージャ > *グローバル*タブの上部では、*新しいウィンドウでメールマネージャを開く*ボタンをクリックしてメールマネージャを開くことができます。

*下部にある統計概観*エリアには、ユニットに現在保存されているすべてのメッセージの概要が表示されます。データはSMTPプロトコル経由かPOP3プロトコル経由かによって分類されています。両方のタイプに対して、次の情報が表示されます。

- 配信待ち *スプール中* (SMTPのみ):スキャン中なのでまだ配信できないなどの理由により、現在スプールにあるメール。
- *クリーンメール*総数(POP3のみ):ユニットがプリフェッチし、クライアント/ユーザがまだ回収していないメール。
- 隔離 *マルウェア*:ウイルスやその他の危険なコンテンツなどのマルウェアを含むメッセージの総数。
- 隔離 *スパム*:スパムと特定されたメッセージの総数。
- 表現*ブロックによる*隔離:許可されない表現が含まれるために隔離に移されたメッセージの総数。

- *ファイル拡張子による隔離*：疑わしい添付ファイルが含まれるために隔離されたメッセージの総数（ファイル拡張子で識別）。
- *スキャン不可のため隔離*：スキャンできないため隔離されたメッセージの総数。
- **MIME**タイプによる隔離（SMTPのみ）：SMTP設定に従ってフィルタすべきMIMEタイプが含まれるため隔離されたメッセージの総数。
- *総隔離数*：隔離されたメッセージの総数。

注 – *配信待ち*の数は、SMTPメッセージの場合はリアルタイムのスナップショットを表します。ただしPOP3メッセージの場合は、表示される数は、前回プリフェッチが有効にされたときからの累積数です。

下に、過去24時間以内のSMTP隔離および拒否（リジェクト）の簡単な統計が表示されます。

- *マルウェア隔離/リジェクト*：有害なコンテンツが含まれるため隔離/拒否されたメッセージの数。
- *スパム隔離/リジェクト*：スパム認定されたため隔離/拒否されたメッセージの数。
- *ブラックリストリジェクト*：送信者がブラックリストに含まれているため拒否されたメッセージの数。
- *アドレス検査リジェクト*：送信者アドレスを検証できなかったため拒否されたメッセージの数。
- **SPF** リジェクト：送信ホストが許可されないため拒否されたメッセージの数。
- **RBL** リジェクト：送信者がリアルタイムブラックホールリストに含まれているため拒否されたメッセージの数。
- **BATV** リジェクト：BATVタグを検証できなかったために拒否されたメッセージの数。
- **RDNS/HELO** リジェクト：HELOが無効であるかRDNSエントリが不足しているために拒否されたメッセージの数。

拒否があるかどうかは*Eメールプロテクション > SMTP*での設定に依存します。

10.7.3 設定

*メールマネージャ > 設定*タブでは、データベースログをどれくらいの期間保存するのか、そして隔離メッセージを何日後に隔離場所から削除するのかを設定することができます。有効期限設定の日数を超えたログとメッセージは自動的に削除されます。

デフォルト設定は次のとおりです。

- データベースログは3日経過後に削除されます。許可される最大日数は30日です。
- 隔離メッセージは14日経過後に削除されます。許可される最大日数は999日です。

データベースログと隔離の両方に対して許可される最低日数は1日です。

データベースログのクリア

このオプションは、データベースログに大量のデータが蓄積された場合にログを即時消去するときに便利です。これを使用すれば、通常のクリーンアップアクションが実行されるまで待つ必要はありません。

11 エンドポイントプロテクション

*エンドポイントプロテクション*メニューでは、エンドポイント、つまりデスクトップコンピュータ、サーバ、ラップトップなどのデバイスの保護を管理することができます。UTMは、エンドポイントソフトウェアの導入、保護対象のエンドポイントの概要確認、エンドポイントのグループ化、ウイルス対策およびデバイスコントロールポリシ、グループポリシの設定、定義したポリシのエンドポイントグループへの割り当てを行うエンドポイント保護の設定サイドです。

エンドポイントプロテクションでは、Sophos LiveConnectと呼ばれるセンターサービスを使用しています。このクラウドベースのサービスは、エンドポイントプロテクションを有効にした段階で、UTMに使用できるように自動的にセットアップされます。LiveConnectを使用すると、ローカルネットワークに存在するかどうかに関係なく、リモートサイトや外出の多いユーザのエンドポイントを含め、常にすべてのエンドポイントを管理できます。LiveConnectサービスは以下を提供します。

- エンドポイントエージェント用の設定済みインストールパッケージ
- エンドポイントに対するポリシの導入および更新
- エンドポイントのセキュリティ更新および定義
- WebAdminによりエンドポイントを集中管理でモニタリングするための中央でのログ記録とデータレポート

LiveConnectはクラウドベースのサービスであるため、サービスを機能させるためには、アクティブなインターネット接続が必要になります。管理対象のエンドポイントにも、ポリシおよびセキュリティ更新を受信するためのインターネット接続が必要になります。

次の図は、LiveConnectサービスを使用したSophos UTMエンドポイントプロテクションの導入例を示しています。
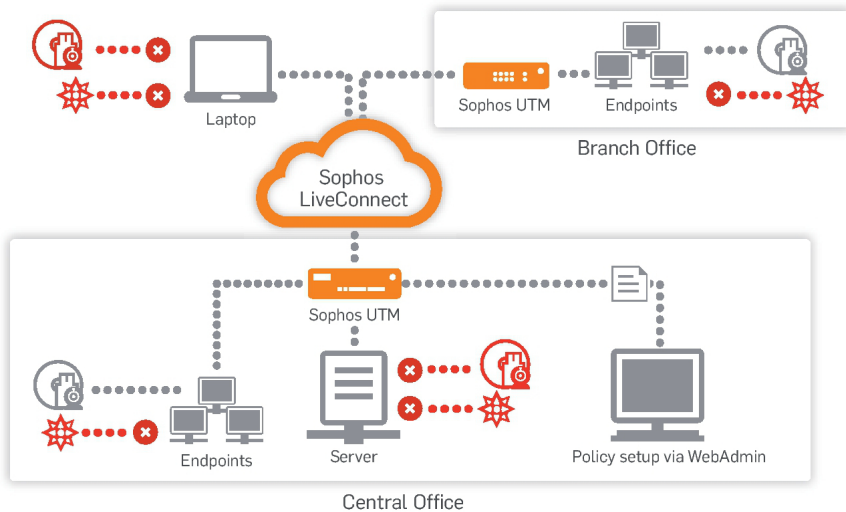
図 **21** エンドポイントプロテクション：概要

この章には次のトピックが含まれます。

- コンピュータ管理
- ウイルス対策
- デバイスコントロール
- Webコントロール

エンドポイントプロテクションを有効にすると、登録されているコンピュータの全般的な情報とステータスを概要ページで確認できます。さらに、リストの並べ替えと検索を行うことができます。エンドポイントのステータスに問題がある場合、ステータスをクリックすると、*詳細*情報を表示することができます。ステータス*非互換*は、デバイスの現在の設定がUTMでの設定と同じでないことを示しています。この問題を解決するために、現在のエンドポイントの設定をエンドポイントに送信するリンクがウィンドウにあります。他のステータスの場合は、情報を確認し、取るべき措置を判断することができます。

エンドポイントプロテクションライブログを開く

エンドポイントプロテクションライブログは、エンドポイント、LiveConnect、UTMの間での接続情報、ならびにエンドポイントに関するセキュリティ情報を提供します。*エンドポイントプロテクションライブログを開く*ボタンをクリックすると、新しいウィンドウでエンドポイントプロテクションライブログが開きます。

11.1 コンピュータ管理

*エンドポイントプロテクション > コンピュータ管理*ページでは、Sophos UTMに接続された個々のコンピュータの保護を管理することができます。

ここでは、エンドポイントのインストールファイルを検索して導入したり、エンドポイントプロテクションソフトウェアがインストールされているすべてのコンピュータの概要を確認することができます。さらに、コンピュータグループに異なるプロテクション設定を定義できます。

11.1.1 グローバル

*エンドポイントプロテクション > コンピュータ管理 > グローバル*タブでは、エンドポイントプロテクションを有効または無効にできます。

エンドポイントプロテクションを有効にするには、次の手順に従います。

1. ***グローバル*タブで、エンドポイントプロテクションを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、組織の詳細に関する一部のフィールドが表示されます。

2. **組織の詳細を入力します。**
   デフォルトで、*マネジメント > システム設定 > 組織*タブの設定が使用されます。

3. **オプションで、親プロキシを設定する:**
   使用しているUTMが直接HTTPでインターネットへアクセスできない場合、エンドポイントプロテクションはプロキシサーバを使用してSophos LiveConnectに到達することができます。*親プロキシを使用*を選択し、必要に応じてホストとポートを入力します。

   ***エンドポイントプロテクションのアクティベート*をクリックします。**
   トグルスイッチが緑色になり、エンドポイントプロテクションが有効になります。
4. 設定をキャンセルするには、アンバー色のトグルスイッチをクリックします。

*エージェントの導入*ページで、モニタリングするコンピュータにエンドポイントプロテクションのインストールパッケージを導入できるようになります。

> **注 –** エンドポイントプロテクションを使用する場合、エンドポイントがインターネットにある更新サーバからデータをダウンロードする際のアップリンク飽和を防ぐために、*Web キャッシング*セク

ションの*Web*プロテクション> *フィルタオプション*> *その他*タブで*Sophosエンドポイントの更新でキャッシングを強制する*機能を有効にすることを推奨いたします。

注 – 管理者は、*管理* > *通知* > *通知*タブのセクション*エンドポイント*で、エンドポイントのウイルス検出用の警告を設定することができます。

注 – Webフィルタが有効で、透過プロキシモードで動作している場合、エンドポイントが適切にエンドポイントプロテクションを使用できることを確認するための追加設定が必要になります。エンドポイントプロテクションを有効にした時点で、UTMにより*Sophos LiveConnect*というDNSグループが自動的に作成されます。このDNSグループを、*Webプロテクション*> *フィルタオプション*> *その他*タブにある*スキップする宛先ホスト/ネット*ボックスに追加します。

エンドポイントプロテクションを無効にするには、次の手順に従います。

1. ***グローバル*タブで、エンドポイントプロテクションを無効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、2つのオプションが使用可能になります。

2. **エンドポイントのデータを削除するかどうかを選択します。**
   すべてのデータを保持する: 一時的にエンドポイントプロテクションを無効にしたい場合は、このオプションを使用します。エンドポイントの設定は保持されます。機能を再度有効にすると、以前にインストールしたエンドポイントが自動的に再接続され、すべての定義済みポリシが使用可能になります。

   すべてのデータを削除する: すべてのエンドポイントの設定をリセットして、最初から始めたい場合はこのオプションを使用します。すべてのエンドポイントへの接続とすべてのポリシ設定が削除されます。再度機能を有効にした後、エンドポイントの新しいインストールパッケージを導入して、新しい登録データを取得します（*コンピュータ管理* > *詳細*のセクションを参照）。

3. ***エンドポイントプロテクションを無効にする*をクリックします。**
   トグルスイッチがグレーになり、エンドポイントプロテクションが無効になります。

11.1.2 エージェントの導入

エンドポイントプロテクション> *コンピュータ管理* > *エージェントの導入*タブでは、エンドポイントプロテクションによりモニタリングする個々のコンピュータ用のインストールファイルを導入できます。

このパッケージで、エンドポイントプロテクションのソフトウェアをエンドポイントに導入する2つの異なる方法があります。

- *今すぐエンドポイントのインストールパッケージをダウンロード*ボタンをクリックして、インストールパッケージをダウンロードして保存します。エンドポイントユーザは、これによりパッケージにアクセスできます。
- 灰色のボックスに表示されたURLをコピーして、エンドポイントユーザに送信します。このURLを使用すると、エンドポイントユーザは自分でインストールパッケージをダウンロード、インストールすることができます。

注 – インストールパッケージの名前は変更しないでください。インストール時に LiveConnect は、このパッケージ名とUTM の現在登録されているデータを比較します。情報が一致しないと、インストールは中止されます。

エンドポイントへのインストール後には、各コンピュータが *コンピュータ管理*タブに表示されます。さらに、*詳細*タブで定義されるコンピュータグループに自動的に割り当てられます。

注 – *詳細*タブの*登録トークンのリセット*ボタンを使用してインストールパッケージを無効にすることができます。

11.1.3 コンピュータの管理

エンドポイントプロテクション > *コンピュータ管理* > *コンピュータの管理*タブでは、UTMのエンドポイントプロテクションがインストールされているコンピュータの概要を表示することができます。コンピュータは自動的にリストに追加されます。ここでは、コンピュータのグループへの割り当て、詳細情報の追加、コンピュータのタンパープロテクション設定の変更、リストからのコンピュータの削除を行うことができます。

リストされているコンピュータの設定を編集するには、次の手順に従います。

1. **各コンピュータの*編集*ボタンをクリックします。**
   *コンピュータの編集*ダイアログボックスが開きます。

2. **次の設定を行います。**
   コンピュータグループ: コンピュータを割り当てるコンピュータグループを選択します。コンピュータは、割り当てられたグループのプロテクション設定を受信します。

   タイプ: コンピュータタイプを選択します（例、デスクトップ、ラップトップ、サーバなど）。タイプによりリストをフィルタすることができます。

タンパープロテクション: 有効にすると、各コンピュータのプロテクション設定をローカルに変更するために、パスワードの入力が必要になります。このパスワードは、*詳細*タブで定義します。無効にすると、エンドポイントユーザはパスワードがなくてもプロテクション設定を変更できます。デフォルトでは、この設定とコンピュータが属するグループの設定が一致します。

資産管理#(オプション):コンピュータの資産管理番号を入力します。

コメント(オプション):説明などの情報を追加します。

3. ***保存*をクリックします。**
   設定が保存されます。

コンピュータをリストから削除するには、*削除*ボタンをクリックします。

注 – コンピュータをリストから削除すると、コンピュータはUTMにより保護されなくなります。ただし、インストール済みのエンドポイントソフトウェアが自動的にアンインストールされることはないので、導入したポリシは有効のままです。

11.1.4 グループ管理

エンドポイントプロテクション > *コンピュータ管理* > *グループの管理*タブでは、保護されたコンピュータをグループ化し、そのグループに対してエンドポイントプロテクション設定を定義することができます。グループに属するすべてのコンピュータには、同じウイルス対策ポリシとデバイスポリシが適用されます。

注 – すべてのコンピュータは一つのグループに所属します。最初は、すべてのコンピュータがデフォルトグループに属します。グループの追加後、*詳細*タブでデフォルトとなるグループ、つまり新しくインストールしたコンピュータを自動的に割り当てるグループを定義できます。

コンピュータグループを作成するには、次の手順に従います。

1. ***コンピュータグループの追加*をクリックします。**
   *コンピュータグループの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:このグループを説明する名前を入力してください。

   ウイルス対策ポリシ:グループに適用するウイルス対策ポリシを選択します。ポリシは、*ウイルス対策* > *ポリシ*タブで定義します。*ウイルス対策* > *除外*タブでこのポリシからの除外をグループごとに定義できます。

デバイスポリシ: グループに適用するデバイスポリシを選択します。ポリシは、*デバイスコントロール* > *ポリシ*タブで定義します。*デバイスコントロール* > *除外*タブでこのポリシからの除外をグループごとに定義できます。

タンパープロテクション: 有効にすると、各エンドポイントのプロテクション設定をローカルに変更するために、パスワードの入力が必要になります。このパスワードは、*詳細*タブで定義します。無効にすると、エンドポイントユーザはパスワードがなくてもプロテクション設定を変更できます。*コンピュータの管理*タブでは、個々のコンピュータのタンパープロテクション設定を変更できます。

Web コントロール: 有効にすると、このグループのエンドポイントは、たとえSophos UTMネットワークになくても、Webフィルタリングポリシを強制、レポートすることができます。エンドポイントWebコントロールを有効にするには、*エンドポイントプロテクション* > ***Web** コントロール*タブを参照してください。

自動更新でプロキシを使用する: 有効にすると、下のフィールドで指定されたプロキシの属性が、このグループのエンドポイントに送信されます。エンドポイントは、このプロキシデータを使用してインターネットに接続します。

> 注 – 正しいデータを入力していることを確認してください。エンドポイントが間違ったプロキシデータを受信すると、これ以降、インターネットやUTMに接続できなくなります。この場合、影響を受けるそれぞれのエンドポイントの設定を手動で変更しなければなりません。

アドレス: プロキシのIP アドレスを入力します。

ポート: プロキシのポート番号を入力します。

ユーザ: 必要に応じて、プロキシのユーザ名を入力します。

パスワード: 必要に応じて、プロキシのパスワードを入力します。

コンピュータ: グループに含めるコンピュータを追加します。

コメント(オプション): 説明などの情報を追加します。

3. ***保存*をクリックします。**
   グループが作成され、*グループの管理*リストに表示されます。すべてのコンピュータが再設定されるまで、15分ほどかかる場合があることに注意してください。

グループを編集または削除するには、対応するボタンをクリックします。

11.1.5 詳細

*エンドポイントプロテクション > コンピュータ管理 > 詳細*タブでは、次のオプションを設定できます。

タンパープロテクション: タンパープロテクションが有効な場合、エンドポイントでプロテクション設定を変更できるのは、このパスワードを使用する場合だけです。

デフォルトコンピュータグループ: エンドポイントプロテクションをインストールしたすぐ後に、自動的にコンピュータが割り当てられるコンピュータグループを選択します。

Sophos LiveConnect – 登録: このセクションには、エンドポイントプロテクションの登録情報が表示されます。その中で、インストールパッケージを特定するために情報が使用され、サポート目的でも使用されます。

Sophos Enterprise Consoleを使用してエンドポイントを管理している場合、このUTMUTMを使用してWebコントロールポリシを提供することができます。*SEC情報*で、*ホスト名*と*共有鍵*を、Sophos Enterprise ConsoleのWebコントロールポリシエディタにコピーします。

- 登録トークンのリセット: このボタンをクリックすると、以前に導入したインストールパッケージでエンドポイントがインストールされることを防ぎます。通常は、展開を完了するためにこれを行います。新しいエンドポイントをインストールしたい場合は、*エージェントの導入*タブで新しいインストールパッケージを指定します。

親プロキシ: UTMUTMが直接インターネットアクセスを持たない場合、親プロキシを使用します。

11.2 ウイルス対策

*エンドポイントプロテクション > ウイルス対策*ページでは、エンドポイントプロテクション機能のウイルス対策設定を定義できます。ウイルス対策ポリシー(つまり、一連のウイルス対策設定)を作成し、後で、これをコンピュータグループに適用し、エンドポイントプロテクションでモニタリングすることができます。さらに、特定のコンピュータグループに適用するウイルス対策機能の例外を定義することもできます。

11.2.1 ポリシー

*エンドポイントプロテクション > ウイルス対策 > ポリシー*タブでは、一連のウイルス対策設定を管理できます。その後ポリシーをコンピュータグループに適用してエンドポイントプロテクションでモニタリングすることができます。

デフォルトでは、*基本プロテクション*ウイルス対策ポリシーが使用できます。これを使用すると、脅威に対するコンピュータの防護と全般的なシステムパフォーマンスの間で最も良好なバランスが得られます。変更はできません。

ウイルス対策ポリシーを追加するには、次の手順に従います。

1. ***ポリシーの追加*ボタンをクリックします。**
   *ポリシーの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前：このポリシを説明する名前を入力します。

   オンアクセススキャン：これを有効にすると、ファイルをコピーまたは移動したり、開くたびに、ファイルがスキャンされ、コンピュータに脅威を及ぼさない場合、または使用が許可されている場合にのみアクセスが許可されます。

   - **PUA**をスキャン：これを有効にすると、オンアクセススキャンの一環でPUA（望ましくないアプリケーション）がないかチェックされます。

   自動クリーンアップ：これを有効にすると、ウイルスまたはスパイウェアを含むアイテムがクリーンアップされ、純粋なマルウェアのアイテムが削除され、感染したアイテムのウイルス駆除が行われます。ウイルススキャナは以前に含まれていたファイルの内容が破損しているかどうかを把握できないため、ウイルス駆除を行ったこれらのファイルは、永久的に破損しているものとみなす必要があります。

   Sophos Live Protection：エンドポイントコンピュータのウイルス対策スキャンでファイルが疑わしいと判断されても、コンピュータに保存されているSophosIDE（脅威ID）ファイルでファイルがクリーンなファイルか悪意のあるファイルかを特定できない場合、詳細な分析を行うために、特定のファイルデータ（チェックサムやその他の属性など）がSophosに送信されます。

   クラウド内チェックは、SophosLabsデータベースで疑わしいファイルの即時ルックアップを実施します。ファイルをクリーンなファイルまたは悪意のあるファイルと特定した場合は、コンピュータにその判定が送り返され、ファイルのステータスが自動的に更新されます。

- サンプルファイルの送信：ファイルが疑わしいとみなされても、ファイルのデータだけでは、確信を持って悪意のあるファイルと特定できない場合、Sophosでファイルのサンプルに対するリクエストを許可することができます。このオプションを有効にすると、既にそのファイルのサンプルが Sophos にない場合、ファイルが自動的に送信されます。サンプルファイルを送信することで、Sophosでは誤検出を行うことなく、マルウェア検出を継続的に改善することができます。

疑わしい動作検出 **HIPS** ：これを有効にすると、レジストリへの疑わしい書き込み、ファイルのコピーアクション、バッファオーバーフロー技術などのアクティブなマルウェアの兆候がないか、すべてのシステムプロセスがモニタリングされます。疑わしいプロセスはブロックされます。

Webプロテクション：これを有効にすると、感染WebサイトのSophosオンラインデータベースでWebサイトのURLが検索されます。

- 悪意のあるサイトブロック：これを有効にすると、悪意のあるコンテンツのサイトがブロックされます。
- ダウンロードスキャン：これを有効にすると、ウイルス対策スキャンによりダウンロード中のデータをスキャンし、ダウンロードに悪意のあるコンテンツが含まれる場合はブロックします。

スケジュールスキャン：これを有効にすると、指定した時刻にスキャンが実施されます。

- ルートキットスキャン：これを有効にすると、各スケジュールスキャンでルートキットがないか、コンピュータがスキャンされます。
- 低優先順位スキャン：これを有効にすると、オンデマンドによるスキャンが低優先順位で実行されます。これが機能するのは、Windows Vista Service Pack 2以降です。
- タイムイベント：エンドポイントのタイムゾーンを考慮して、スキャンを実施するタイムイベントを選択します。

コメント(オプション)：説明などの情報を追加します。

3. *保存*をクリックします。
   新しいポリシーがウイルス対策ポリシーリストに表示されます。設定の変更後にすべてのコンピュータが設定されるまで、15分ほどかかる場合があることに注意してください。

ポリシーを編集または削除するには、対応するボタンをクリックします。

11.2.2 除外

*エンドポイントプロテクション > ウイルス対策 > 除外*タブで、エンドポイントプロテクションのウイルス対策設定からの除外をコンピュータグループごとに定義できます。除外を設定すると、ウイルス対策ポリシー設定のために行われるスキャンからアイテムが除外されます。

除外を追加するには、次の手順に従います。

1. ***除外*タブで、*除外の追加*をクリックします。**
   *除外リストの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   タイプ: オンアクセススキャンおよびオンデマンドスキャンからスキップするアイテムのタイプを選択します。

   - *アドウェアと***PUA**: これを選択すると、スキャンとブロックから特定のソフトウェアまたはPUA(望ましくないアプリケーション)を除外できます。アドウェアは、ユーザーの生産性やシステム効率に影響を与える可能性のある広告(ポップアップメッセージなど)を表示します。PUAは悪意あるソフトウェアではないものの、一般的にビジネスネットワークに不適切とみなされています。*ファイル名*フィールドに、`example.stuff` などのアドウェアや PUAの名前を追加します。

   - *ファイル/フォルダ*: これを選択すると、アンチウイルススキャンからファイル、フォルダ、ネットワークドライブを除外できます。*ファイル/パス*フィールドに、`C:\Documents\` や `\\Server\Users\Documents\CV.doc` など、ファイル、フォルダ、またはネットワークドライブを入力します。

   - *ファイル拡張子*: これを選択すると、特定拡張子のファイルを追加し、ウイルス対策スキャンをすることができます。*拡張子*フィールドに、`html`などの拡張子を入力します。

   - *バッファオーバーフロー*: これを選択すると、バッファオーバーフロー技術を使用するアプリケーションが動作モニタリングでブロックされるのを防止することができます。オプションで、*ファイル名*フィールドにアプリケーションファイル名を入力したり、*アップロード*フィールドでファイルをアップロードします。

   - *疑わしいファイル*: これを選択すると、疑わしいファイルがウイルス対策スキャンでブロックされるのを防止することができます。*アップロード*フィールドでファイルをアップロードします。UTMは、ファイルのMD5チェックサムを生成します。アップロードされたファイルの名前は、自動的に*ファイル名*フィールドで使用されます。オプションで、ファイル名を変更することも可能です。ファイルのファイル名が定義されていて、保存さ

れたMD5チェックサムがクライアントで見つかれば、ウイルス対策スキャンでブロックされることはありません。

- 疑わしいふるまい: これを選択すると、ファイルが疑わしいふるまい検知でブロックされるのを防止することができます。オプションで、*ファイル名*フィールドにファイル名を入力したり、*アップロード*フィールドでファイルをアップロードします。
- **Web**サイト: これを選択すると、*Web フォーマット*フィールドで指定したプロパティと一致するWebサイトはウイルス対策プロテクションでスキャンされません。

  Webフォーマット: 閲覧を許可するWebサイトのサーバを指定します。

  - ドメイン名 : 許可するドメインの名前を*Web サイト*フィールドに入力します。
  - **IP**アドレスとサブネットマスク: 許可するコンピュータのIPv4アドレスとネットマスクを入力します。
  - **IP**アドレス: 許可するコンピュータのIPv4アドレスを入力します。

アップロード(*バッファオーバーフロー*、*疑わしいファイル*、および*疑わしいふるまいのタイプのみ*) : ウイルス対策スキャンからスキップするファイルをアップロードします。

コンピュータグループ: この除外を有効にするコンピュータグループを選択します。

コメント(オプション) : 説明などの情報を追加します。

3. ***保存*をクリックします。**
   新しい除外ルールが*除外*リストに表示されます。

除外ルールを編集または削除するには、対応するボタンをクリックします。

11.3 デバイスコントロール

*エンドポイントプロテクション > デバイスコントロール*ページでは、エンドポイントプロテクションによりモニタリングするコンピュータに接続されたデバイスを制御できます。基本的には、ポリシが割り当てられたコンピュータグループに対して許可またはブロックするデバイスのタイプをデバイスポリシで定義します。デバイスを検出すると、エンドポイントプロテクションは各コンピュータのコンピュータグループに適用されているデバイスポリシに従って、デバイスが許可されているかどうかをチェックします。デバイスポリシでブロックまたは制限が指定されている場合は、デバイスが*除外*タブに表示され、ここでデバイスの除外を追加することができます。

11.3.1 ポリシー

エンドポイントプロテクション > *デバイスコントロール* > *ポリシー*タブでは、一連のデバイスコントロール設定を管理できます。その後これをコンピュータグループに適用してエンドポイントプロテクションでモニタリングすることができます。これらの設定は、デバイスポリシーと呼ばれています。

デフォルトでは、2種類のデバイスポリシが用意され、*すべてブロック*ではあらゆるタイプのデバイスの使用を禁止し、*フルアクセス*ではすべてのデバイスに対するすべての権限を許可します。これらのポリシは変更できません。

新しいポリシーを追加するには、以下の手順に従います。

1. ***ポリシーの追加*ボタンをクリックします。**
   *ポリシーの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:このポリシを説明する名前を入力します。

   ストレージ機器:各種ストレージ機器に対して、*許可*または*ブロック*を設定できます。該当する場合は、*読取専用*エントリも選択できます。

   ネットワーク機器:モデムおよびワイヤレスネットワークには、*許可*、*ブリッジをブロック*、*ブロック*のいずれかを選択できます。

   短距離通信機器:Bluetoothや赤外線機器に対して、*許可*または*ブロック*を設定できます。

3. コメント(オプション):説明などの情報を追加します。

4. ***保存*をクリックします。**
   新しいポリシがデバイスコントロールリストに表示されます。これをコンピュータグループに適用することができます。設定の変更後にすべてのコンピュータが設定されるまで、15分ほどかかる場合があることに注意してください。

ポリシーを編集または削除するには、対応するボタンをクリックします。

11.3.2 除外

エンドポイントプロテクション > *デバイスコントロール* > *除外*タブでは、デバイスに対するプロテクションの除外を設定することができます。除外を指定すると、コンピュータグループに割り当てられたデバイスポリシによって禁止されているものが常に許可されます。除外はコンピュータのグループに対して行われるため、除外は必ず選択したグループのすべてのコンピュータに適用されます。

*除外*リストには、適用されているデバイスコントロールポリシによりブロックまたはアクセス制限が行われている検出済みデバイスが自動的にすべて表示されます。技術的に識別できないフロッピードライブの場合、複数のフロッピードライブが接続されていると、1つのエントリのみが表示され、これがすべてのフロッピードライブのプレースホルダとして機能します。

デバイスの除外を追加するには、次の手順に従います。

1. **デバイスの*編集*ボタンをクリックします。**
   *デバイスの編集*ダイアログボックスが開きます。

2. **次の設定を行います。**
   許可：このデバイスを許可するコンピュータグループを追加します。

   読取専用/ブリッジ：読み取り専用モード（ストレージ機器に適用）またはブリッジモード（ネットワーク機器に適用）でこのデバイスを許可するコンピュータグループを追加します。

   全てに適用：このオプションを選択すると、デバイスIDが同じすべてのデバイスに現在の設定が適用されます。これは、たとえば同じタイプの複数のUSBスティックのセットに一般的な除外を割り当てたい場合などに役立ちます。

   モード: このオプションは、*全てに適用*チェックボックスを選択解除している場合にだけ使用可能です。この場合、何が他に一般的除外を持つデバイスになるかを指定する必要があります。影響を受けるデバイスに対して一般的除外を保持したい場合は、*他のために保持*を選択します。一般的除外を削除したい場合は、*他のために削除*をクリックします。

   ヒント – 一般的除外の例に関する詳細情報は、下の一般的デバイス除外を操作するのセクションを参照してください。

   コメント（オプション）：説明などの情報を追加します。

3. ***保存*をクリックします。**
   編集したデバイスについて、コンピュータのグループ、ならびにそれらの除外が表示されます。

注 – デバイスが一度*除外*リストに存在すると、*削除*ボタンを使用して削除するまでリストに残ります。通常、対応するハードウェアデバイスを完全に取り外してから（例、もう存在しない光学ドライブ）、あるいはデバイスポリシを変更してから（例、ワイヤレスネットワークアダプターを一般に許可）、デバイスを削除します。まだ使用しているデバイスを削除すると、*OK*で確認する必要があるメッセージボックスが表示されます。その後、デバイスがリストから削除されます。そのデバイスに対して除外が存在する場合、除外は自動的に無効になります。例、現在のデバイスポリシがそのデバイスに適用されます。

一般的デバイス除外を操作する

一般的デバイス除外とは、同じデバイスIDを持つすべてのデバイスに自動的に適用される除外です。

一般的除外の作成

1. 一般的除外を持たないデバイスの*編集*ボタンをクリックします。例、*全てに適用*チェックボックスが選択解除されます。
2. 除外を設定して、*全てに適用*チェックボックスを選択します。
3. **除外を保存します。**
   同じデバイスIDを持つすべてのデバイスに除外が適用されます。

一般的な除外対象からデバイスを外す

1. 既存の一般的除外から除外したいデバイスの*編集*ボタンをクリックします。
2. 個別の除外を設定して、*全てに適用*チェックボックスを選択解除します。
3. モードドロップダウンリストで、*他のために保持*を選択します。
4. **除外を保存します。**
   編集されたデバイスは個別の除外を持ちますが、他は一般的除外のままになります。

一般的除外を持つすべてのデバイスの設定を変更する

1. 一般的除外を持つデバイスの**1**つについて、*編集*ボタンをクリックします。
2. *全てに適用*チェックボックスを選択したまま、除外を設定します。
3. **除外を保存します。**
   *全てに適用*チェックボックスが選択されている、同じデバイスIDを持つすべてのデバイスの設定がこれに従って変更されます。

一般的除外の削除

1. 一般的除外を持つデバイスの**1**つについて、*編集*ボタンをクリックします。
2. *全てに適用*チェックボックスを選択解除します。
3. モードドロップダウンリストで、*他のために削除*を選択します。
4. **除外を保存します。**
   *全てに適用*チェックボックスが選択されている、同じデバイスIDを持つすべてのデバイスの除外が削除されます。編集されたデバイスだけが、引き続き個別の除外を持ちます。

11.4 エンドポイントWebコントロール

Sophos UTMは、企業ネットワーク内からWebのブラウジングを行うシステムに対してセキュリティと生産性保護を提供し、エンドポイントWebコントロールはこの保護をユーザのマシンに拡張します。これは、企業ネットワークの内外に位置したり、ローミングを行うエンドポイントのマシンに対して、プロテクション、コントロール、レポートを提供します。有効にすると、*Webプロテクション > Webフィルタリング*や*Webプロテクション > Webフィルタプロファイル > プロキシプロファイル*で定義されるすべてのポリシが、たとえコンピュータがUTMネットワークになくても、エンドポイントWebコントロールによって強制されます。Sophos UTMとSophosエンドポイントは、LiveConnectを通じて通信します。LiveConnectは、インスタントポリシを有効にし、Sophos UTMとシームレスに通信し、Sophosエンドポイントをローミングして更新をレポートするクラウドサービスです。たとえば、家庭やコーヒーショップでラップトップをローミングすると、Webコントロールポリシを強制し、Sophos UTMはローミングしたラップトップからのログ情報を受け取ります。

11.4.1 グローバル

*エンドポイントプロテクション > Webコントロール > グローバル*タブでは、エンドポイントWebコントロールを有効または無効にできます。エンドポイントWebコントロールのフィルタリングポリシを設定するには、*エンドポイントプロテクション > コンピュータ管理 > グループ管理*ページで関連するグループについてWebコントロールが有効であり、そのグループが*Webプロテクション > Webフィルタプロファイル > プロキシプロファイル*タブでプロキシプロファイルによって参照されていることが必要です。

11.4.2 詳細

*エンドポイントプロテクション > Webコントロール > 詳細*タブで、*通信をゲートウェイとエンドポイントでスキャンする*を選択できます。また、関連する割当てを有するサイトに遭遇した場合に、エンドポイントWebコントロールが行うべきアクションを設定できます。

エンドポイントトラフィック設定

デフォルトでは、Sophos UTMは、Webコントロールが有効であるエンドポイントに対してはWebトラフィックをスキャンしません。このオプションを選択すると、エンドポイントとSophos UTMの両方がWebトラフィックをフィルタします。

エンドポイント割当てアクション

Sophos Endpoint Webコントロールは時間割当てを強制できません。関連する割当てを有するサイトのエンドポイントについては、別のアクションを選択します。

注 – エンドポイント設定が優先されます。例えば、エンドポイントWebコントロールが有効化され、*通信をゲートウェイとエンドポイントでスキャンする*が選択され、*エンドポイント割当てアクション*が*警告*に設定されている場合、ユーザは最初に警告を受けます。サイトへと進むと、そのサイトの割当て時間の利用状況が効力を持つようになります。エンドポイント割当てアクションが*ブロック*に設定されている場合、そのサイトの割当て時間を有しているユーザであってもブロックされます。

11.4.3 サポートされていない機能

Web コントロール機能をエンドポイントに拡張するメリットは多数ありますが、Sophos UTM ネットワークのみで使用できる機能もあります。Sophos UTMでは対応しているが、エンドポイント Web コントロールでは対応していない機能は次のとおりです。

- **HTTPS SSL** トラフィックのスキャン: HTTPSトラフィックは、エンドポイントではスキャンできません。エンドポイントがプロキシ経由で UTM を使用している場合、この機能が有効化されていると、トラフィックは UTM によってスキャンされます。
- 認証モード: エンドポイントは、必ず現在ログオンしているユーザー(SSO)を使用します。エンドポイントは認証を実行できません。エンドポイントを移動先で使用している場合、UTM に接続して認証することはできません。
- ウイルス対策/マルウェア対策: Sophosエンドポイントのウイルス対策設定は*エンドポイントプロテクション > ウイルス対策*ページで行われます。Web プロテクション (ダウンロードスキャン) を有効にしている場合、すべての Web コンテンツに対して、常にウイルスのシングスキャンを実行します。デュアルスキャンおよび最大スキャンサイズには対応していません。
- アクティブコンテンツ削除
- **YouTube for Schools**
- ストリーミング設定: Sophosエンドポイントは、必ずストリーミングコンテンツのウイルスをスキャンします。
- スキャンできないファイル、暗号化されたファイルのブロック
- ダウンロードサイズでブロック
- 許可されるターゲットサービス: この機能は、Sophos UTMだけに適用されます。

- **Web キャッシング**: この機能は、Sophos UTMだけに適用されます。

12 ワイヤレスプロテクション

*ワイヤレスプロテクション*メニューを使用して、Sophos UTMのワイヤレスアクセスポイント、対応するワイヤレスネットワーク、ワイヤレスアクセスを利用するクライアントを設定および管理することができます。アクセスポイントはUTM上で自動的に設定されるため、個別に設定する必要はありません。アクセスポイントの設定およびステータス情報を交換するために使UTM用される、とアクセスポイントの間の通信は、AESを使用して暗号化されます。

重要 – アクセスポイントが激しく点滅している場合は、電源を切断しないでください。激しい点滅は、ファームウェアフラッシュが現在行われていることを意味します。ファームウェアフラッシュは、ワイヤレスプロテクション更新に伴うUTMシステム更新の後などに実行されます。

この章には次のトピックが含まれます。

- グローバル設定
- ワイヤレスネットワーク
- メッシュネットワーク
- アクセスポイント
- ワイヤレスクライアント
- ホットスポット

ワイヤレスプロテクションの概要ページは、接続されたアクセスポイント、そのステータス、接続されたクライアント、ワイヤレスネットワーク、メッシュネットワーク、メッシュピアリンクに関する基本情報を示します。

*現在接続されている*セクションでは、エントリをSSID またはアクセスポイントによってソートし、左にある折りたたみアイコンをクリックして、個々のエントリを展開したり、折りたたんだりすることができます。

ライブログ

*ワイヤレスプロテクションライブログを開く*ボタンをクリックすると、アクセスポイントおよび接続を試行するクライアントに関する詳細な接続およびデバッグ情報が表示されます。

12.1 グローバル設定

*ワイヤレスプロテクション > グローバル設定*ページでは、ワイヤレスプロテクションの有効化、ワイヤレスプロテクションおよびWPA/WPA2エンタープライズ認証用のネットワークインタフェースの設定が可能です。

12.1.1 グローバル設定

*ワイヤレスプロテクション > グローバル設定 > グローバル設定*タブで、ワイヤレスプロテクションを有効または無効にできます。

ワイヤレスプロテクションを有効にするには、次の手順に従います。

1. ***グローバル設定*タブで、ワイヤレスプロテクションを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、*アクセスコントロール*エリアが編集可能になります。

   ワイヤレスプロテクションを初めて有効にする際は、*初期セットアップ*セクションが表示されます。ここには、作成される設定が表示されています。WPA2個人暗号化をDHCP用ワイヤレスクライアントで使用する個別のワイヤレス「ゲスト」ネットワーク。および*Webサーフィン*サービスでUTMのDNSを使用することが許可されます。事前共有鍵は自動生成され、このセクションのみに表示されます。初期設定はテンプレートとして機能します。いつでも*ワイヤレスプロテクション > ワイヤレスネットワーク*ページで設定を編集することができます。

   自動設定のスキップ: また、このオプションを選択して、初期セットアップをスキップすることもできます。この場合、ワイヤレス設定を手動で設定する必要があります。

2. **アクセスポイント用のネットワークインタフェースを選択します。**
   アクセスポイントをプラグインする設定済みインタフェースを選択するには、*許可されるインタフェース*セクションのフォルダアイコンをクリックします。DHCPサーバーがこのインタフェースに関連付けられていることを確認してください。

   > **注 –** UTM「w」の印が付いているアプライアンス(例えばSG 105–125w)は、ネットワークを選択する必要がありません。これらのアプライアンスはWifiカードが装備されているため、専用のWiFiインタフェースが必要ありません。

3. ***適用*をクリックします。**

設定が保存されます。トグルスイッチが緑色になり、ワイヤレスプロテクションが有効になります。

設定されたネットワークインタフェースにアクセスポイントをプラグインして、続行することができます。自動設定のスキップを選択した場合は、*ワイヤレスネットワーク*ページで設定を続けます。

設定をキャンセルするには、アンバー色のトグルスイッチをクリックします。

アクセスポイントをプラグインするとすぐに、アクセスポイントはシステムに自動的に接続します。新たに接続された未設定のアクセスポイントは、*アクセスポイント* > *概要*ページで*保留中のアクセスポイント*としてリストされます。

12.1.2 詳細

ワイヤレスプロテクション > *グローバル設定* > *詳細*タブでは、WPA/WPA2エンタープライズ認証を使用しオフラインアクセスポイントの遅延通知を指定するよう、アクセスポイントを設定することができます。

エンタープライズ認証

エンタープライズ認証には、RADIUSサーバのいくつかの情報を入力する必要があります。APは認証のためにRADIUSサーバと通信せず、UTMとだけ通信します。UTMとAPの間のRADIUS通信にはポート`414`が使用されます。

> **注 –** RADIUSサーバーがIPsecトンネル経由でUTMに接続されている場合、通信が正確に行わるよう徹底させるため、追加のSNATルールを設定しなければなりません。*ネットワークプロテクション* > *NAT* > *NAT*タブで、以下のSNATルールを追加します:APのネットワークからのトラフィック、サービスRADIUSを使用するトラフィック、およびRADIUSサーバーに向かうトラフィックについては、ソースアドレスを、RADIUSサーバー到達に使用されるUTMのIPアドレスに置き換える。

要求のRADIUSサーバーをドロップダウンリストから選択します。サーバは、*定義とユーザ* > *認証サービス* > *サーバ*で追加および設定可能です。

> **注 –** RADIUSサーバーがIPsecトンネル経由でUTMに接続されている場合、通信が正確に行わるよう徹底させるため、追加のSNATルールを設定しなければなりません。*ネットワークプロテクション* > *NAT* > *NAT*タブで、以下のSNATルールを追加します:APのネットワークからのトラフィック、サービスRADIUSを使用するトラフィック、およびRADIUSサーバーに向かうトラフィックについては、ソースアドレスを、RADIUSサーバー到達に使用されるUTMのIPアドレスに置き換える。

設定を保存するには*適用*をクリックします。

通知のタイムアウト

アクセスポイントがオフラインである場合、通知が送付されます。通知のタイムアウトにより、通知のタイムアウト時間を設定できます。これは、例えば遅延を2分に設定すると、アクセスポイントが少なくとも2分間オフラインになった場合に通知が送付されます。通知のタイムアウトは整数でなければなりません。デフォルトのタイムアウトは5分です。

通知のタイムアウトを設定するは、次の手順に従います。

1. タイムアウト値を分で入力します。
2. ***適用*をクリックします。**
   設定が保存されます。

12.2 ワイヤレスネットワーク

ワイヤレスプロテクション > *ワイヤレスネットワーク*ページでは、ワイヤレスネットワークを定義できます(SSIDおよび暗号化方式など)。さらに、ワイヤレスネットワークに個別のIPアドレス範囲が必要か、アクセスポイントのLANに対するブリッジングが必要かを定義することができます。

新しいワイヤレスネットワークを作成するには、次の手順に従います。

1. ***ワイヤレスネットワーク*ページで*ワイヤレスネットワークの追加*をクリックします。**
   *ワイヤレスネットワークの追加*ダイアログボックスが開きます。
2. **次の設定を行います。**
   ネットワーク名:ネットワークを説明する名前を入力します。

   ネットワーク**SSID**: ワイヤレスネットワークの識別のためにクライアントに表示される、ネットワークのサービスセット識別子(SSID)を入力します。SSIDは、1～32文字のASCII印字可能文字[1]で構成します。コンマは使用できず、先頭または末尾をスペースにすることはできません。

   暗号化モード:ドロップダウンリストから暗号化モードを選択します。デフォルトは*WPA 2パーソナル*です。できる限り、*WPA*よりも*WPA2*を使用することをお勧めします。セキュリティ上の理由から、ワイヤレスネットワークを使用しているクライアントの中に、WEP以外の方法をサポートしないクライアントがいなければ、WEPを使用しないことを推奨します。エンター

---

[1] http://en.wikipedia.org/wiki/ASCII#ASCII_printable_characters

プライズ認証方式を使用する場合、*グローバル設定* > *詳細*タブでRADIUSサーバも設定する必要があります。RADIUSサーバのNAS IDとして、ワイヤレスネットワーク名を入力します。

> **注 –** UTMはWPA2(PSK/エンタープライズ)ネットワークのIEEE 802.11r標準をサポートしてローミング時間を低減します。クライアントも、IEEE 802.11r標準をサポートする必要があります。

パスフレーズ/**PSK**: *WPA/WPA2 パーソナル*暗号化モードのみで使用できます。許可されないアクセスからワイヤレスネットワークを保護するパスフレーズを入力し、次のフィールドに再入力してください。パスフレーズには、8～63文字のASCII印字可能文字を使用します。

128 ビットの**WEP**キー: *WEP*暗号化モードのみで使用できます。ここで、26文字ちょうどの16進文字から成るWEPキーを入力します。

クライアントトラフィック: ワイヤレスネットワークをローカルネットワークに統合する方法を選択します。

- 分離ゾーン(デフォルト):ワイヤレスネットワークは、独自のIPアドレス範囲を持つ独立したネットワークとして処理されます。このオプションを使用する場合、ワイヤレスネットワークを追加した後に、次のセクション(分離ゾーンネットワークの次のステップ)の手順に従ってセットアップを継続する必要があります。

  > **注 –** 既存の*別ゾーン*ネットワークを*AP LANへのブリッジ*または*VLANへのブリッジ*に切り替えると、UTM上の設定済みWLANインタフェースは*未割り当て*になります。ただし、編集して再有効化することにより、新しいハードウェアインタフェースをインタフェースオブジェクトに割り当てることができます。

- **AP**の**LAN**にブリッジ:ワイヤレスネットワークをアクセスポイントのネットワークにブリッジングすることができます。つまり、無線LANクライアントは同じIPアドレス範囲を共有します。

  > **注 –** VLANが有効な場合、無線LANクライアントはアクセスポイントのVLANネットワークにブリッジングされます。

- **VLAN**にブリッジ:このワイヤレスネットワークのトラフィックを任意のVLANにブリッジングさせることができます。これは、ワイヤレスクライアントから独立した共通ネット

ワーク内にアクセスポイントを含めたい場合に便利です。

VLAN IDにブリッジ: ワイヤレスクライアントが含まれるネットワークのVLAN IDを入力します。

クライアント**VLAN ID**(*エンタープライズ*暗号化モードのみで使用可能): VLAN IDの定義方法を選択します:

- *スタティック*: *VLAN IDにブリッジ*フィールドに定義されたVLAN IDを使用します。
- **RADIUS**および*スタティック*: RADIUSサーバが提供するVLAN IDを使用します。ユーザがいずれかのワイヤレスネットワークに接続し、RADIUSサーバで認証を行うと、RADIUSサーバはこのユーザに対して使用すべきVLAN IDをアクセスポイントに知らせます。したがって、複数のワイヤレスネットワークを使用する際に、どのユーザがどの内部ネットワークにアクセスできるのかをユーザごとに定義することができます。ユーザにVLAN ID属性が割り当てられていない場合、*VLAN IDへのブリッジ*フィールドで定義されたVLAN IDが使用されます。

- スタンドアロンインタフェース(ローカルWifiデバイスのみ): Wifi装備のSG「w」アプライアンスについては、ワイヤレスネットワークを直接UTM上で設定できます。IPアドレス範囲を設定できるほか、標準イーサネットデバイスのようなDHCPを設定できます。インタフェースは「WirelessBridgebr10X」という名のブリッジに隷属し、*インタフェース& ルーティング > インタフェース > インタフェース*タブにリストされます。

コメント(オプション): 説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**

アルゴリズム(WPA/WPA2暗号化モードでのみ使用可能): 暗号化アルゴリズムを*AES*または*TKIP*。セキュリティ上の理由から、*AES*を使用することをお勧めします。

周波数帯: このワイヤレスネットワークに割り当てられたアクセスポイントは選択した周波数帯で送信を行います。5 GHz帯は、通常パフォーマンスが高い一方で、レイテンシが低く、一般的に干渉も少なくなっています。したがって、VoIP通信などに優先使用するようにしてください。AP 50のみで5 GHz帯での送信が可能です。

タイムベースアクセス: タイムスケジュールに応じてワイヤレスネットワークを自動的に有効/無効にするには、このオプションを選択します。

有効な時間帯の選択: ワイヤレスネットワークを有効にする時間を定義した時間帯定義を選択します。「+」アイコンをクリックして新しい時間帯定義を追加できます。

クライアント隔離：ネットワーク内のクライアントは通常、互いに通信できます。ゲストネットワーク内などでこれを禁止したい場合、ドロップダウンリストで*有効*を選択します。

SSID非表示：SSIDを非表示にしたい場合があります。これには、ドロップダウンリストから*はい*を選択します。これはセキュリティ機能ではありません。

高速移行（WPA2パーソナル/エンタープライズ暗号化モードのみで利用可能）：WWPA2暗号化付きワイヤレスネットワークは、IEEE 802.11r標準を使用します。これを防止するには、ドロップダウンリストから*無効化*を選択します。

MAC フィルタリングタイプ: このワイヤレスネットワークにアクセスできるMACアドレスを制限するには、*ブラックリスト*または*ホワイトリスト*を選択します。*ブラックリスト*を使用する場合、以下の MAC アドレスリストで指定したものを除く、すべての MAC アドレスが許可されます。*ホワイトリスト*を使用する場合、以下の MAC アドレスリストで指定したものを除く、すべての MAC アドレスがブロックされます。

MACアドレス: ワイヤレスネットワークへのアクセスを制限するために使用されるMACアドレスのリスト。MACアドレスリストは、*定義とユーザ* > *ネットワーク定義* > *MAC アドレス定義*タブで作成できます。最大で200のMACアドレスを使用できます。

4. ***保存*をクリックします。**
   設定が保存されます。ワイヤレスネットワークが *ワイヤレスネットワークリストに表示されます。*

別ゾーンネットワークの次のステップ

*別ゾーン*オプションを指定してワイヤレスネットワークを作成した場合、*wlan0*のように、対応する新しい仮想ハードウェアインタフェースが自動的に作成されます。このワイヤレスネットワークを使用するためには、更なる手動設定が必要になります。次の手順で実行します：

1. **新しいネットワークインタフェースを設定します。**
   インタフェース& ルーティング > *インタフェース* > *インタフェース*タブで新しいインタフェースを作成し、ハードウェアとしてwlanインタフェース（wlan0など）を選択します。タイプが「イーサネット」であることを確認し、ワイヤレスネットワークのIPアドレスとネットマスクを指定します。

2. **ワイヤレスクライアントのDHCPを有効にします。**
   クライアントがUTMに接続できるようにするためには、クライアントにIPアドレスとデフォルトゲートウェイを割り当てる必要があります。そのため、*ネットワークサービス* > *DHCP* > *サーバ*タブで、このインタフェースにDHCPサーバをセットアップします。

3. **ワイヤレスクライアントのDNSを有効にします。**

クライアントがDNS名を解決できるようにするためには、クライアントがDNSサーバにアクセスできるようにする必要があります。*ネットワークサービス > DNS > グローバル*タブで、許可ネットワークリストにインタフェースを追加します。

4. **ワイヤレスネットワークをマスクするNATルールを作成します。**
その他のネットワークと同様に、ワイヤレスネットワークのアドレスをアップリンクインタフェースのアドレスに変換する必要があります。*ネットワークプロテクション > NAT > マスカレード*タブでNATルールを作成します。

5. **1つ以上のパケットフィルタルールを作成して、ワイヤレスネットワークとのトラフィックの送受信を許可します。**
その他のネットワークと同様に、1つ以上のパケットフィルタルールを作成して、WebサーフィントラフィックなどのトラフィックがUTMを通過できるようにします。*ネットワークプロテクション > ファイアウォール > ルール*タブでパケットフィルタルールを作成します。

12.3 アクセスポイント

*ワイヤレスプロテクション > アクセスポイント*ページは、システムで認識されているアクセスポイント(AP)の概要を示します。ここでは、APの属性の編集、APの削除またはグループ化、APまたはAPグループへのワイヤレスネットワークの割り当てを行うことができます。

注 – ベーシックガードサブスクリプションでは、に接続できるアクセスポイントは1つだけです UTM。アクセスポイントの最大数は、UTMアプライアンスによって223に制限されています。

アクセスポイントのタイプ

現在Sophosは、以下の専用アクセスポイントを提供しています。

- AP 5:802.11b/g/n規格、2.4 GHz帯

  USBコネクタでRED rev2またはrev3に接続することだけが可能であり、WLANタイプが*AP LANにブリッジ*であるSSIDを1つと最大で7のワイヤレスクライアントを正確にサポートします。

- AP 10:802.11b/g/n規格、2.4 GHz帯

- AP 15:802.11b/g/n規格、2.4 GHz帯

  AP 15には、使用できるチャネルが異なる2つのモデルがあります。

- FCC規制準拠ドメイン(主に米国):チャネル1～11
    - ETSI規制準拠ドメイン(主に欧州):チャネル1～13

- AP 30:802.11b/g/n規格、2.4 GHz帯
- AP 50:802.11a/b/g/n規格、2.4/5 GHzデュアルバンド/デュアルラジオ

  AP 50には、使用できるチャネルが異なる2つのモデルがあります。

    - FCC規制準拠ドメイン(主に米国):チャネル1～11、36～48、149～165
    - ETSI規制準拠ドメイン(主に欧州):チャネル1～13、36～48

- AP 100:802.11a/b/g/n規格、2.4/5 GHzデュアルバンド/デュアルラジオ

  AP 100には、使用できるチャネルが異なる2つのモデルがあります。

    - FCC規制準拠ドメイン(主に米国):チャネル1～11、36～48、149～165
    - ETSI規制準拠ドメイン(主に欧州):チャネル1～13、36～64、100～116、132～140

Sophosは、以下の統合アクセス機能付きSGアプライアンスも提供しています。

- SG 105w/115w:802.11a/b/g/n規格、2.4/5 GHzデュアルバンド
- SG 125w/135w:802.11a/b/g/n規格、2.4/5 GHzデュアルバンド

APの国設定によって、各地の法律に準拠するために使用できるチャネルが決まりますので、ご注意ください。

クロスリファレンス – アクセスポイントに関する詳細情報は、Sophos UTMリソースセンターにある*取扱説明書*を参照してください。

12.3.1 概要

*ワイヤレスプロテクション > アクセスポイント > 概要*ページは、システムで認識されているアクセスポイント(AP)の概要を示します。Sophos UTMは、アクティブ、インアクティブ、保留中のAPを識別します。本物のAPのみがネットワークに接続するようにするためには、最初にAPを承認する必要があります。

注 – AP 5を使用する場合は、最初にREDマネジメントを有効にして、REDをセットアップします。その後、REDインタフェースが*ワイヤレスプロテクション > グローバル設定*ページの許可インタフェースに追加されていることを確認します。AP 5をREDに接続した後は、AP 5が*保留中のアクセスポイント*セクションに表示されるはずです。

アクセスポイントは*グループ化*タブで一時的に無効にすることができます。APをネットワークから物理的に削除する場合は、ここで*削除*ボタンをクリックして削除します。APがネットワークに接続されている限り、削除後も*保留中*状態で自動的に再表,示されます。装備WiFi機能付きのSG「w」アプライアンスはAPリストから削除できません。

ヒント – このページの各セクションは、セクションヘッダの右にあるアイコンをクリックして、折りたたみ/展開できます。

アクティブなアクセスポイント

ここには、接続、設定が完了し稼働中のAPがリストされます。APを編集するには、*編集*ボタンをクリックします(下の*アクセスポイントの編集*を参照)。

インアクティブなアクセスポイント

ここには、過去に設定済みで現在はUTMに接続されていないAPがリストされます。APがこの状態で5分間経過した場合、APのネットワーク接続とシステムの設定を確認してください。ワイヤレスプロテクションサービスを再起動すると、*最後の表示*タイムスタンプが消去されます。APを編集するには、*編集*ボタンをクリックします(下の*アクセスポイントの編集*を参照)。

保留中のアクセスポイント

ここには、システムに接続されているが未承認のAPがリストされます。アクセスポイントを承認するには、*同意*ボタンをクリックします(下の*アクセスポイントの編集*を参照)。

設定を受信すると、認可済みのアクセスポイントが、現在アクティブであるか否かに応じて、上のいずれかのセクションに即時に表示されるようになります。

アクセスポイントの編集

1. **各アクセスポイントの*編集*または*承諾*ボタンをクリックします。**
   *アクセスポインの編集*ダイアログウィンドウが開きます。

2. **次の設定を行います。**
   ラベル(オプション):ネットワークのAPを簡単に特定するためにラベルを入力します。

   国:APが設置された国を選択します。お使いのSGアプライアンス(ローカルWifiデバイス)に組み込まれているAPの国は、*マネジメント*> *システム設定* > *組織*タブのグローバル国設定から生成されます。

重要 – 国設定により、送信に使用できるチャネルが決まります。各地の法律に準拠するために、正しい国を選択してください(*アクセスポイント*の章を参照してください)。

グループ化(オプション):APをグループ別に編成することができます。以前にグループを作成している場合は、ドロップダウンリストから選択できます。それ以外の場合は、<<*新規グループ*>>を選択し、*名前*テキストボックスに表示されるグループ名を入力します。グループは、*グループ化*タブで編成できます。

3. ***ワイヤレスネットワーク*セクションで、以下の設定を行います**:
ワイヤレスネットワークの選択(グループまたは新しいグループが選択されていない場合のみ):アクセスポイントがブロードキャストする必要があるワイヤレスネットワークを選択します。これは、オフィスにのみブロードキャストすべき会社のワイヤレスネットワークや、建物内の公共部分のみでブロードキャストすべきゲストワイヤレスネットワークなどで便利です。リストヘッダのフィルタフィールドを使用して、ワイヤレスネットワークを検索することができます。

注 – ワイヤレスネットワークをブロードキャストするアクセスポイントは、特定の条件を満たさなければなりません。そうした条件については、下のAPへのネットワーク割り当てのルールのセクションを参照してください。

4. **オプションで、*メッシュネットワーク*セクションで、以下の設定を行います** AP 50でのみ使用可能であり、*メッシュネットワーク*タブでメッシュネットワークが定義されている場合にだけ使用可能 :
メッシュロール:「+」アイコンをクリックして、アクセスポイントによってブロードキャストされるべきメッシュネットワークを選択します。ダイアログウィンドウが開きます。
   - メッシュ: メッシュネットワークを選択します。
   - ロール:選択したメッシュネットワークでのアクセスポイントのロールを定義します。ルート アクセスポイントは、UTM に直接接続しています。初期設定を受信したメッシュ アクセスポイントは、UTM から切断されたら、メッシュネットワーク経由でルートアクセスポイントに接続します。各アクセスポイントは、1つのメッシュネットワークに対してのみメッシュ アクセスポイントとして機能できることに注意してください。

保存すると、*メッシュロール*リストのアクセスポイントアイコンがアクセスポイントのロールを示します。機能アイコンによって、メッシュロールを編集したり、リストから削除したりすることができます。

重要 – *メッシュロール*リストからメッシュロールを削除する場合、初期構成を得るにはアクセスポイントを再度イーサネットにつなぐ必要があります。アクセスポイントを再度イーサネットにつなぐ必要なしでメッシュネットワークを変更するには、メッシュロールを削除するのではなく、代わりに、メッシュロールの編集アイコンをクリックして、必要なメッシュネットワークを選択します。

5. **次の詳細設定を任意で行います。**
帯域(ローカルWiFiデバイスでのみ利用可能):ローカルWiFiデバイスで設定できるのは1つの帯域のみです。ドロップダウンリストから*5 GHz*または*2.4 GHz*を選択します。

チャネル(ローカルWiFiデバイスでのみ利用可能):最後の送信に使用したチャネルを選択する場合は、デフォルト設定の*自動*のままにします。または、固定チャネルを選択します。

送信出力(ローカルWiFiデバイスでのみ利用可能):アクセスポイントで最大出力で送信するには、デフォルト設定の*100 %*のままにします。または、干渉を低減するためなど、作動距離を短縮するには出力を低減します。

*チャネル***2.4 GHz**: デフォルト設定の*自動*のままにすると、送信で一番使用されていないチャネルが自動的に選択されます。または、固定のチャネルを選択します。

動的*チャネル*: 選択されている場合、APはすべての利用可能なチャネルをスキャンし、最良のシグナル強度のチャネルに接続します。

タイムベーススキャン: 選択されている場合、APは定期的に最良のシグナル強度のチャネルをチェックします。タイムイベントを追加するには、「+」アイコンをクリックしてタイムデータを入力します。また、*定義とユーザ* > *期間定義*タブにリストされている定義済みのタイムイベントを選択することも可能です。

*チャネル***5 GHz**(AP 50でのみ使用可能):デフォルト設定の*自動*のままにすると、送信で一番使用されていないチャネルが自動的に選択されます。あるいは、固定チャネルを選択することもできます。

ヒント–*自動*を選択すると、現在使用されているチャネルが、アクセスポイントのエントリでアナウンスされます。

送信出力**2.4 GHz**: アクセスポイントで最大出力で送信するためには、デフォルト設定の*100 %*のままにすることができます。干渉を低減するためなど、作動距離を短縮するためには出力を低減することができます。

送信出力**5 GHz**（AP 50のみで使用可能）：AP 50では、5 GHz帯の送信出力を個別に低減することができます。

STP: スパニングツリープロトコルを有効化するには、ドロップダウンリストから*有効*を選択します。このネットワークプロトコルは、ブリッジのループを検出して回避します。アクセスポイントがメッシュネットワークをブロードキャストする場合は、STPが必須です。

VLANタギング：VLANタギングはデフォルトでは無効になっています。APを既存のVLANイーサネットインタフェースに接続するには、チェックボックスにチェックを入れて、VLANタギングを有効にする必要があります。VLANイーサネットインタフェースが、*グローバル設定* > *グローバル設定*ページの*許可ネットワーク*ボックスに追加されていることを確認します。

注 – ネットワーク内のアクセスポイントに対してVLANの使用を導入するには、以下の手順に従います。標準LANを使用して、APをUTMに1分以上接続します。これは、APが設定を取得するために必要です。最初からVLAN経由で接続すると、APはVLAN内にあることを認識しないため、設定を取得するためにUTMに接続することができません。APが表示されたら、VLANを有効にしてVLAN IDを入力します。その後、APを目的のVLAN（スイッチなど）に接続します。

注 – AP 5では、VLANタギングができません。

AP VLAN ID：*VLANタギング*が有効な場合、UTMアクセスポイントがに接続するために使用するVLANのVLANタグを入力します。VLAN タグ `0` および `1` は使用しないでください。一般に、これらのタグはネットワークハードウェア（スイッチなど）上で特別な意味を持ちます。通常、`4095` は管理用として予約されています。

注 – VLANタギングが設定されている場合、APは設定されたVLANに対してDHCPを60秒間試行します。この時間内にIPアドレスを受信できなかった場合、APはフォールバックとして標準のLANでDHCPを試みます。

6. ***保存*をクリックします。**
アクセスポイントは、それぞれ設定または設定の更新を受信します。

注 – 設定の変更後、すべてのインタフェースが再設定されるまで約15秒必要です。

VLANタギングが設定されており、APがVLAN経由でUTMにコンタクトできない場合、APは自動的にリブートし、設定の受信後に再試行します。

APへのネットワーク割り当てのルール

ワイヤレスネットワークの*クライアントトラフィック*オプションとアクセスポイントの*VLANタギング*オプションが適合する場合にのみ、アクセスポイントをワイヤレスネットワークに割り当てることができます。この際、次のルールが適用されます。

- クライアントトラフィックが*別ゾーン*のワイヤレスネットワーク:アクセスポイントのVLANタギングを有効または無効にすることができます。
- クライアントトラフィックが*APのLANにブリッジ*のワイヤレスネットワーク:アクセスポイントのVLANタギングを無効にする必要があります。
- クライアントトラフィックが*VLANにブリッジ*のワイヤレスネットワーク:アクセスポイントのVLANタギングを有効にする必要があります。それぞれのワイヤレスクライアントは、ワイヤレスネットワークに指定された*VLAN IDにブリッジ*を使用するか、RADIUサーバでVLAN IDが指定されている場合は、RADIUSサーバからを受信します。

注 – AP 5 は、*クライアントトラフィック*オプションが*AP LANにブリッジ*の1つのワイヤレスネットワークにのみ割り当てることができます。

ブリック済みAPの再フラッシュ

アクセスポイントが返される主な理由は、破損したファームウェアでデバイスがブリックされているからです。そのため、Sophosアクセスポイントを再フラッシュするツールをダウンロード可能です。当該ツールは、ここに用意されています。

ツールをWindows 8上で実行する場合、まずWindows Firewallを無効にする必要があります。

Sophosアクセスポイントを再フラッシュするには、次の手順に従います。

1. **AP再フラッシュユーティリティをダウンロードします。**
2. **ダウンロードしたファイルを解凍します。**
3. **exe-ファイルをアドミニストレータとして実行して、再フラッシュユーティリティを起動します。**
4. **指示に従って、APデバイスをフラッシュします。**
   電源LEDが即座にフラッシュします。

電源LED毎秒フラッシュするようになったら、プロセスは完了です。

ブリック済みREDデバイスの再フラッシュ

ツールをダウンロードして、SophosRED10デバイスを再フラッシュできます。当該ツールは、ここに用意されています。

ツールをWindows 8上で実行する場合、まずWindows Firewallを無効にする必要があります。

SophosREDを再フラッシュするには、次の手順に従います。

1. 再フラッシュユーティリティをダウンロードします。
2. ダウンロードしたファイルを解凍します。
3. **exe-**ファイルをアドミニストレータとして実行して、再フラッシュユーティリティを起動します。
4. **指示に従って、REDデバイスを再フラッシュします。**
   フラッシュするまで約2分間かかります。

12.3.2 グループ化

ワイヤレスプロテクション > *アクセスポイント* > *グループ化*ページでは、複数の方法でアクセスポイント(AP)を管理することができます。このリストは、すべてのアクセスポイントのグループおよびグループ化されていないアクセスポイントの概要を提供します。アクセスポイントとグループは、それぞれのアイコンで区別できます。

アクセスポイントのグループを作成するには、次の手順に従います。

1. ***グループ*ページで、*新規グループ*をクリックします。**
   *新規アクセスポイントグループ*ダイアログボックスが開きます。
2. **次の設定を行います。**
   名前:このアクセスポイントのグループを説明する名前を入力してください。

   VLANタギング:**VLAN**タギングはデフォルトでは無効になっています。APを既存のVLANイーサネットインタフェースに接続するには、チェックボックスにチェックを入れて、VLANタギングを有効にする必要があります。VLANイーサネットインタフェースが、*グローバル設定* > *グローバル設定*ページの*許可ネットワーク*ボックスに追加されていることを確認します。

   AP VLAN ID:UTMへの接続でこの**AP**のグループによって使用される**VLAN**のタグを入力します。VLANタグ`0`および`1`は使用しないでください。一般に、これらのタグはネットワークハードウェア(スイッチなど)上で特別な意味を持ちます。通常、`4095`は管理用として予約されています。

アクセスポイントの選択:グループのメンバになる必要があるアクセスポイントを選択します。他のグループに割り当てられていないアクセスポイントだけが表示されます。

注 – ローカルWiFiデバイスはグループ化できません。また、アクセスポイントの選択には表示されません。ローカルWiFiデバイスは、*グループ化*リストに表示されます。

ワイヤレスネットワークの選択:このグループのアクセスポイントによってブロードキャストされる必要があるワイヤレスネットワークを選択します。

注 – ワイヤレスネットワークをブロードキャストするアクセスポイントは、特定の条件を満たさなければなりません。そうした条件については、*アクセスポイントの* > *概要*の章のAPへのネットワーク割り当てのルールのセクションを参照してください。

3. ***保存*をクリックします。**
   新しいアクセスポイントのグループが、*グループ化*リストに表示されます。

グループを編集または削除するには、対応するグループのボタンをクリックします。

アクセスポイントを編集または削除するには、対応するアクセスポイントのボタンをクリックします。アクセスポイントの編集や削除に関する詳細情報は、*アクセスポイントの* > *概要*の章を参照

12.4 メッシュネットワーク

ワイヤレスプロテクション > *メッシュネットワーク*画面では、メッシュネットワークを定義し、ブロードキャストの対象となるアクセスポイントを関連付けることができます。一般的には、メッシュネットワークでは、複数のアクセスポイントが互いに通信し、共通ワイヤレスネットワークでブロードキャストします。一方、メッシュネットワークで接続されているアクセスポイントは同じワイヤレスネットワークでクライアントにブロードキャストすることができるので、広いエリアをカバーしながら、単一のアクセスポイントとして機能することもできます。他方、メッシュネットワークはケーブルを敷設することなくイーサネットネットワークをブリッジすることができます。

メッシュネットワークで関連付けられたアクセスポイントは、2つの役割の1つを果たすことができます: ルートアクセスポイントまたはメッシュアクセスポイントのどちらかです。どちらもメッシュネットワークをブロードキャストできるので、ブロードキャストできる他方のワイヤレスネットワークの量が1つ減ります。

- *ルートアクセスポイント*: UTMに有線接続され、メッシュネットワークを提供します。アクセスポイントは、複数のメッシュネットワークのルートアクセスポイントになることができます。

- メッシュアクセスポイント: メッシュネットワークは、UTMルートアクセスポイント経由でに接続される必要があります。アクセスポイントがメッシュアクセスポイントになることができるメッシュネットワークは、一度に1つだけです。

メッシュネットワークは、2つの主な使用例で使用できます:ワイヤレスブリッジまたはワイヤレスリピータを実装できます:

- ワイヤレスブリッジ:2つのアクセスポイントを使用して、2つのイーサネットセグメント間でワイヤレス接続を確立できます。イーサネットセグメントを接続するケーブルを敷設できない場合に、ワイヤレスブリッジが便利です。UTMでの最初のイーサネットセグメントはルートアクセスポイントのイーサネットインターフェースに接続されますが、2番目のイーサネットセグメントはメッシュアクセスポイントのイーサネットインターフェースに接続する必要があります。複数のメッシュアクセスポイントを使用して、さらにイーサネットセグメントを接続することができます。
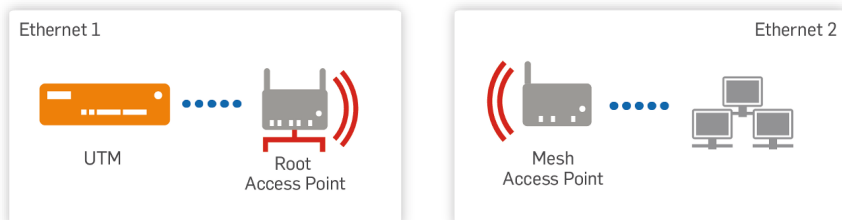
図 **22** メッシュネットワーク使用例ワイヤレスブリッジ

- ワイヤレスリピータ: のイーサネットは、UTMルートアクセスポイントのイーサネットインターフェースに接続されます。ルートアクセスポイントには、メッシュネットワーク経由でのメッシュアクセスポイントへのワイヤレス接続があり、ワイヤレスネットワークをワイヤレスクライアントへブロードキャストします。
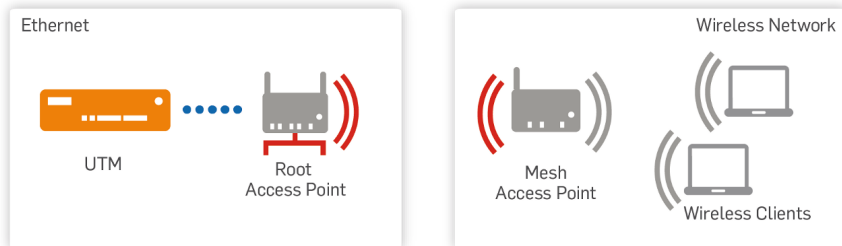
図 **23** メッシュネットワーク使用例ワイヤレスリピータ

新しいメッシュネットワークを定義するには、次の手順に従います。

1. *メッシュネットワーク***ページで、***メッシュネットワークの追加***をクリックします。**
   *メッシュネットワークの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   メッシュID : メッシュネットワークに一意のIDを入力します。

   周波数帯 : このネットワークに割り当てられたアクセスポイントは選択した周波数帯でメッシュネットワークに送信を行います。一般的には、ブロードキャストされるワイヤレスネットワークと異なる周波数帯をメッシュネットワークに使用することをお勧めします。

   コメント(オプション) : 説明などの情報を追加します。

   アクセスポイント: 「+」アイコンをクリックし、メッシュネットワークをブロードキャストするアクセスポイントを選択します。*メッシュのロールの追加*ダイアログウィンドウが開きます。

   - **AP** : アクセスポイントを選択します。ブロードキャストするメッシュネットワークで一度に使用できるアクセスポイントは50までです。
   - ロール : 選択したメッシュネットワークでのアクセスポイントのロールを定義します。ルート アクセスポイントは、UTM に直接接続しています。初期設定を受信したメッシュ アクセスポイントは、UTM から切断されたら、メッシュネットワーク経由でルートアクセスポイントに接続します。各アクセスポイントは、1つのメッシュネットワークに対してのみメッシュ アクセスポイントとして機能できることに注意してください。

   注 – 初期構成では、メッシュアクセスポイントを、*グローバル設定*タブの*許可されるインタフェース*ボックスで選択したイーサネットセグメントの1つにある他のアクセスポイントと同じようにメッシュアクセスポイントとつなぐことが重要です。

   リストからアクセスポイントを削除するには、*アクセスポイント*リストの削除アイコンを使用します。

   重要 – *アクセスポイント*リストからメッシュアクセスポイントを削除する場合、初期構成を得るにはアクセスポイントを再度イーサネットにつなぐ必要があります。アクセスポイントを再度イーサネットにつなぐ必要なしでメッシュネットワークを変更するには、アクセスポイントを削除する代わりに*アクセスポイント > 概要*タブにあるアクセスポイントの*編集*ボタンをクリックし、*メッシュネットワーク*セクションの編集アイコンをクリックし、目的のメッシュネットワークを選択します。

   アクセスポイントアイコンがアクセスポイントのロールを指定します。リストヘッダのフィルタフィールドを使用して、アクセスポイントリスト内を検索することができます。

3. *保存*をクリックします。
   設定が保存されます。メッシュネットワークが*メッシュネットワーク*リストに表示されます。

12.5 ワイヤレスクライアント

*ワイヤレスプロテクション > ワイヤレスクライアント*ページは、現在アクセスポイントに接続されている（または過去に接続されていた）クライアントの概要を示します。

すべてのクライアントが名前を送信する訳ではないため、ここで名前を割り当てて、概要で既知のクライアントを識別しやすくできます。クライアントがDHCP要求中にNetBIOS名を送信する場合、この名前がテーブルに表示されます。送信しない場合、クライアントはリストに*[unknown]*（不明）と表示されます。これらの不明クライアントの名前は、名前の前にある「+」アイコンをクリックして変更することができます。次に、名前を入力して*保存*をクリックします。変更が有効になるまで数秒かかります。WebAdminの右上隅にある*リロード*ボタンから、クライアントの名前を参照できます。名前を変更する場合は、*編集*ボタンをクリックします。

注 – クライアントに名前を追加すると、パフォーマンスに影響がでる場合があります。

また、テーブルにある*削除*アイコンをクリックして、クライアントをテーブルから削除することもできます。

ワイヤレスプロテクションサービスを再起動すると、*最後の表示*タイムスタンプが消去されます。

12.6 ホットスポット

*ワイヤレスプロテクション > ホットスポット*ページでは、キャプティブポータルシステムによりアクセスを管理できます。ホットスポット機能により、カフェ、ホテル、企業などではゲストに時間制限やトラフィック制限を課したインターネットアクセスを提供できます。この機能は、ワイヤレスサブスクリプション内で使用できますが、有線ネットワークでも機能します。

注 – 技術的には、ホットスポット機能により、基本的にファイアウォールで許可されているトラフィックが制限されることになります。したがって、ホットスポットを介してトラフィックを管理できるようにするためのファイアウォールルールを設定していることを確認する必要があります。ホットスポットを有効にする前に、ホットスポット機能を無効にした状態でトラフィックをテストすることをお勧めします。

注 – ホットスポット機能をアクティブ-アクティブのクラスタセットアップとの組み合わせで使用する場合、マスターとワーカーの間でトラフィックを配分することはできません。ホットスポットインタフェースとの間でのすべてのトラフィックは、マスターから流れます。

ホットスポットの生成

最初に管理者は特定タイプのアクセスを備えたホットスポットを作成して有効にする必要があります。次のタイプを使用できます。

- 利用規約の許諾 : ゲストに提示する利用規約を作成できます。ゲストがホットスポットにアクセスするためには、利用規約のチェックボックスにチェックを入れる必要があります。
- 当日有効パスワード: ゲストがホットスポットにアクセスするためには、パスワードを入力する必要があります。パスワードは毎日変更されます。
- バウチャー: ゲストがホットスポットにアクセスするためには、バウチャーを取得してバウチャーコードを入力する必要があります。バウチャーは、デバイスの数、時間、トラフィックで制限することができます。

ゲストへのアクセス情報の配信

*当日有効パスワード*および*バウチャー*タイプでは、アクセス情報をゲストに提供する必要があります。したがって、アクセス情報を管理して配信できるユーザを定義することができます。これらのユーザは、ユーザポータルの*ホットスポット*タブでアクセス情報を受信して配信します。

- 当日有効パスワード: 現在のパスワードはメールで送信したり、ユーザがユーザポータルでパスワードを確認することができます。ユーザはゲストにパスワードを転送します。ユーザは新しいパスワードを生成したり、入力することができます。新しいパスワードを設定すると、古いパスワードが自動的に無効になり、アクティブなセッションが終了します。他のユーザには、それぞれの設定に応じて、メールまたはユーザポータルで新しいパスワードを連絡します。
- バウチャー: ユーザポータルでは、ユーザはそれぞれ一意のコードのバウチャーを作成できます。管理者によって指定されている場合は、異なるタイプのバウチャーを使用できます。バウチャーは印刷したりエクスポートして、ゲストに提供することができます。作成したバウチャーのリストにより、バウチャーの使用状況を把握および管理できます。

法的情報

多くの国では、公共ワイヤレスLANの運用には、国の特定の法律が適用され、法的に疑問のあるコンテンツのWebサイト（ファイル共有サイト、過激派のWebサイトなど）へのアクセスが制限されています。この要件に準拠するためには、ホットスポットにSophos UTMのWebプロテクション機能を組み合わせて、ウェブサイトのカテゴリタイプ全体から1つのURLまでをブロックしたり、許可したりすることで、Webアクセスを制御できます。UTMを使用すると、アクセスの可能なサイトやコンテンツ、ユーザ、アクセス時間を完全に制御することができます。これにより、国や企業のポリシによって義務付けられている場合に、ホットスポットに厳格な制限を課すことができます。

さらに、Sophos UTMの組み込みHTTPプロキシを使用しても、高度なログとレポート機能が得られます。レポートには、誰がどのサイトをいつ、何回閲覧したかが表示されるため、アクセス制限を行わずにホットスポットを運用したい場合でも、不適切な使用を特定することができます。

さらに国によっては、国の規制機関にホットスポットを登録することが義務付けられている場合があります。

12.6.1 グローバル

ワイヤレスプロテクション > *ホットスポット* > *グローバル*タブでは、ホットスポット機能を有効にし、ホットスポットアクセス情報の表示と配信を許可するユーザを定義できます。

ホットスポットを設定するには、次の手順に従います。

1. ***グローバル*タブで、ホットスポットを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチが緑色になり、*グローバルホットスポット設定*エリアが編集可能になります。

2. **許可するユーザを選択します。**
   ユーザポータルを通じてホットスポットアクセス情報を提供できるユーザまたはグループを選択するか、新しいユーザを追加します。ここで選択したユーザは、当日有効パスワードを変更したり、ホットスポットバウチャーを作成できます。ユーザを追加する方法は、*定義とユーザ* > *ユーザとグループ* > *ユーザ*ページで説明しています。

3. ***適用*をクリックします。**
   設定が保存されます。

ライブログ

ホットスポットのライブログには、ホットスポットの使用状況に関する状況が表示されます。*ホットスポットのライブログを開く*ボタンをクリックすると、新しいウィンドウでライブログが開きます。

テンプレートのダウンロード

ここでは、新しいホットスポットを追加する際にデフォルトで使用できるホットスポットログインテンプレートおよびバウチャーテンプレートをダウンロードできます。デフォルトのテンプレートを変更して、ホットスポットのログインページや、スクラッチから作成する必要がないバウチャーの設計をカスタマイズすることができます。カスタマイズしたHTMおよびPDFのテンプレートは、*ワイヤレスプロテクション > ホットスポット > ホットスポット*タブでアップロードします。

1. **青いダウンロードアイコンをクリックします。**
   *証明書ファイルのダウンロード*ダイアログウィンドウが開きます。

2. **ファイルを保存します。**
   ファイルがダウンロードされます。

12.6.2 ホットスポット

*ワイヤレスプロテクション > ホットスポット > ホットスポット*タブでは、各種のホットスポットを管理できます。

注 – ホットスポットは、WLANインタフェースなどの既存のインタフェースに割り当てる必要があります。このインタフェースを使用するすべてのホストは、ホットスポットにより自動的に制限されます。したがって、通常ホットスポットを作成する前にクライアントトラフィックが*別ゾーン*のワイヤレスネットワークを作成してから、各WLANインタフェースハードウェアのインタフェースを作成します。詳しくは、*ワイヤレスプロテクション > ワイヤレスネットワーク*を参照してください。

ホットスポットを作成するには、次の手順に従います。

1. ***ホットスポットの追加*をクリックします。**
   *ホットスポットの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前 : このホットスポットを説明する名前を入力します。

インタフェース: ホットスポットにより制限するインタフェースを追加します。選択したインタフェースに対して、必要なトラフィックを許可するファイアウォールルールが設定されていることを確認してください。インタフェースは、1つのホットスポットでのみ使用できます。

警告 – 後でインターネットへのトラフィックが完全にブロックされるので、ここではアップリンクインタフェースは選択しないでください。さらに、認証などの重要なサービスを提供するサーバが使用しているインタフェースを使用することを強くお勧めします。そうしないと、WebAdminから完全にロックアウトされる可能性があります！

管理ユーザ: 管理設定のユーザを追加または選択します。管理ユーザはユーザポータル内で、バウチャーの作成および当日有効パスワードの変更ができます。デフォルトでは、管理設定を行える人はいません。

HTTPSにリダイレクト: 有効化すると、ユーザはHTTPSにリダイレクトされます。

- ホスト名タイプ: *IPアドレス*または*カスタムホスト名* *DNS* にリダイレクトする場合に選択します。
- ホスト名（カスタムホスト名でのみ利用可能）:リダイレクト用のホスト名を選択または追加します。

ホットスポットタイプ: 選択したインタフェースのホットスポットタイプを選択します。

- 当日有効パスワード: 新しいパスワードが1日に1回自動的に作成されます。このパスワードは、ユーザーポータルの*ホットスポット*タブに表示されます。これは、*グローバル*タブに指定されているすべてのユーザーに提供されます。さらに、指定したメールアドレスに送信されます。
- バウチャー（ベーシックガードサブスクリプションでは使用できません。）:このホットスポットタイプでは、さまざまな制限とプロパティを持つユーザポータルのトークンを作成、印刷してユーザに提供することができます。ユーザがコードを入力すると、インターネットに直接アクセスできます。
- 利用規約の許諾 : ユーザは利用規約を許諾した後にインターネットにアクセスできます。
- バックエンド認証 : このタイプのホットスポットでは、ユーザは任意のサポートされているバックエンドメカニズムで認証できます（*定義とユーザ* > *認証サービス*を参照）。このタイプでは、ユーザの資格情報はユーザの認証状況をチェックするために定期的に保存されます。

- **SMS**認証：このホットスポットタイプを利用すると、携帯電話経由で認証ができます。検証コードはSMS経由で送付され、特定の時間枠内で入力が行われると、アクセスが認められます。
- **MICROS**インタフェース – **FIAS**：このホットスポットを利用すると、MICROS Fidelioシステムをサポートするホテルの名称および部屋番号を経由しての認証が可能です。この認証は、バウチャーでのみ有効です。サーバおよびポートがMICROS Fidelioソフトウェアにより作成/提供されますので、UTMに追加するだけです。

注 – *バックエンド認証*を選択すると、ホットスポットがOTP機能として設定されている場合には、OTPトークンの新しいエントリがログインフォームに表示されます。

パスワード生成時刻（*当日有効パスワード*のホットスポットタイプのみ）：新しいパスワードを作成する指定時刻。この時刻になると、古いパスワードが即時に無効になり、現在のセッションが切断されます。

パスワードのメール送信先（*当日有効パスワード*のホットスポットタイプのみ）：パスワードを送信するメールアドレスを追加します。

バウチャー定義（*バウチャー*のホットスポットタイプのみ）：ホットスポットに使用する定義を選択します。バウチャー定義の追加方法は、*バウチャー定義*ページで説明しています。

バウチャー当たりのデバイス（*バウチャー*、*SMS認証*または*MICROSインタフェース – FIAS*のホットスポットタイプのみ）：バウチャーの有効期間中に1つのバウチャーでログインを許可するデバイス数を入力します。これを*無制限*にすることは推奨されません。

ホットスポットユーザ（ホットスポットタイプの*バックエンド認証*の場合のみ）：バックエンド認証を通じてホットスポットにアクセスできるユーザまたはグループを選択するか、新しいユーザを追加します。一般に、これはバックエンドのユーザグループです。

SMSテキスト（*SMS認証*のホットスポットタイプのみ）：検証SMSのテキストをオンデマンドで変更します。<*?CODE?*>は自動的に、検証コードに置き換えられることに注意してください。

セッション有効期限（*利用規約の許諾*、*SMS認証*または*バックエンド認証*のホットスポットタイプのみ）：アクセスの期限が切れるまでの時間を選択します。*その後*、*利用規約の許諾*のホットスポットタイプで、ユーザは利用規約を受諾してログインする必要があります。*バックエンド認証*のホットスポットタイプで、ユーザは認証しなおす必要があります。

パスワードをワイヤレスネットワーク**PSK**と同期（*当日有効パスワード*のみ）：新しく作成/保存したパスワードをワイヤレスPSKと同期するには、このオプションを選択します。

注 – 新しいPSKにより、分離ゾーンワイヤレスネットワークによって設定されており、またホットスポットインタフェースとして使用されている、すべてのAPが再設定され、再起動されます。これは、すべての接続が途切れるということを意味します。

ユーザに利用規約の許諾を求める（*利用規約の許諾*のホットスポットタイプ以外）：ホットスポットユーザがインターネットにアクセスする前に、ユーザに利用規約を許諾してもらう場合は、このオプションを選択します。

- 利用規約：利用規約として表示するテキストを追加します。シンプルなHTMLマークアップとハイパーリンクを使用できます。

ログイン後にURLへリダイレクト：選択すると、パスワードまたはバウチャーデータを入力した後、ユーザは自動的に特定のURLへリダイレクトされます。例、ホテルのWebサイト、ポータルシステムのポリシを説明しているWebサイトなど。

- **URL**：ユーザがリダイレクトされるURL。

コメント（オプション）：説明などの情報を追加します。

3. **オプションで、以下のホットスポットのカスタマイズ設定を行います。**
デフォルトでは、ユーザにはSophosロゴが付いたログインページが表示されます。カスタマイズされたHTMLファイルを、独自の画像やスタイルシートと共に使用することができます。さらに、バウチャーのレイアウトをカスタマイズすることもできます。

カスタマイズのタイプ：カスタマイズのタイプを選択します。次のタイプを使用できます。

- 基本：デフォルトのログインページテンプレートを使用します。必要であれば、ロゴ、タイトル、テキストを変更します。

  ロゴ：ログインページのロゴをアップロードします。サポートされている画像ファイルのタイプは、jpg、png、gifです。幅300 px、高さ100 pxの最大画像を推奨いたします（タイトルの長さによります）。*デフォルトへリストア*ボタンを使用すると、デフォルトのSophosロゴを再度選択できます。

  ロゴのサイズを推奨サイズにする：選択すると、推奨される幅や高さを超えているロゴが、縮小されて、推奨サイズで表示されます。選択しなければ、ロゴは元のサイズで表示されます。

  タイトル：ログインページにタイトルを追加します。シンプルなHTMLマークアップとハイパーリンクを使用できます。

カスタムテキスト: ログインページに追加テキストを追加します。使用するワイヤレスネットワークのSSIDなどを入力できます。シンプルなHTMLマークアップとハイパーリンクを使用できます。

- *フル*: 個別のログイHTMLページを選択します。

  ログインページテンプレート: 個別のログインページとして使用したいHTMLテンプレートを選択します。フォルダアイコンをクリックすると、ファイルを選択してアップロードすることができるウィンドウが開きます。*デフォルトへリストア*ボタンを使用すると、デフォルトのSophosHTMLテンプレートを再度選択できます。このテンプレートで、それぞれのホットスポットに動的に情報を挿入できる変数を使用できます。たとえば、会社名、管理者情報、利用規約、ログインフォームなどを追加できます。詳細情報は、下記の*ログインページテンプレートでの変数の使用*を参照してください。デフォルトのHTMLのテンプレートは、*ワイヤレスプロテクション* > *ホットスポット* > *グローバル*タブでダウンロードできます。

  画像/スタイルシート: ログインページテンプレートで参照されているファイルを追加します。例、画像、スタイルシート、JavaScriptファイルなど。フォルダアイコンをクリックすると、ファイルを選択してアップロードすることができるウィンドウが開きます。

バウチャーテンプレート（*バウチャー*のホットスポットタイプのみ）: フォルダアイコンをクリックすると、バウチャーレイアウトのPDFファイルを選択してアップロードすることができるウィンドウが開きます。デフォルトでは、デフォルトテンプレートが使用されます。*デフォルトへリストア*ボタンをクリックすると、デフォルトを復元できます。バウチャーPDFファイルは、PDFバージョンPDF 1.5またはそれ以下である必要があります。ページサイズおよびフォーマットは任意です－サイズとフォーマットの両方が、指定されたページサイズおよびページ当たりのバウチャー数に応じて、ユーザポータルでバウチャー作成中に調整されます。デフォルトのPDFのテンプレートは、*ワイヤレスプロテクション* > *ホットスポット* > *グローバル*タブでダウンロードできます。

PDFファイルには、ユーザポータルでのバウチャー生成中にそれぞれの値に置き換えられる、以下の変数を含めることができます:

- ワイヤレスネットワーク名（SSID）: `<?ssid0?>`（および`<?ssid1?>`、`<?ssid2?>`など、WLAN に複数のSSIDがある場合）
- ワイヤレスネットワークのパスワード: `<?psk0?>`（および`<?psk1?>`、`<?psk2?>`など、WLAN に複数のSSIDがある場合）
- バウチャーコード: `<?code?>`
- バウチャー有効時間: `<?validity?>`

- **バウチャーデータ限度**：<?datalimit?>
- **バウチャー時間限度**：<?timelimit?>
- **コメント**：<?comment?>
- ホットスポットアクセスデータがエンコードされたQRコード：<?qrX?>。QRコードの左上隅が、変数の左下隅に配置されます。

注 – 変数を使用する場合、PDFファイルには使用するフォントの完全な文字セットが含まれている必要があります。変数が値と置換されて、代替文字セットの一部が使用できない場合は、正しく表示されません。文字列
<?abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789?>
をPDFファイルに追加することを推奨いたします。この文字列は、バウチャー生成中に自動的に削除されます。さらに、代替テキストが長すぎるとレイアウトが壊れるので、変数には個別の行を使うことを推奨いたします。

4. ***保存*をクリックします。**
ホットスポットが作成され、*ホットスポット*リストに表示されます。

ヒント – ホットスポットを保存した後、ログインページのプレビューを開くことができます。ホットスポットリストで各ホットスポットの*ログインページをプレビューボタンをクリック*するだけです。

ホットスポットを編集または削除するには、対応するボタンをクリックします。

ログインページテンプレートでの変数の使用

ログインページのHTMLテンプレートには、ホットスポットのログインページの情報を動的に挿入できる、さまざまな変数が含まれていることがあります。ログインページを表示するためにUTMがテンプレートを処理すると、一時的変数が関連する値に置換されます。有効な変数：

- 一般的変数

  <?company_text?>：*マネジメント* > *カスタマイズ* > *グローバル*で定義されるカスタムの会社テキスト

  <?company_logo?>：*マネジメント* > *カスタマイズ* > *グローバル*で定義される会社ロゴ。この変数は、ロゴファイルのパスで置換されます。使用例、<img src="<?company_logo?>">

<?admin_contact?>: *マネジメント* > *カスタマイズ* > *Web メッセージ*で定義される管理者の名前またはアドレス

<?admin_message?>: *マネジメント* > *カスタマイズ* > *Web メッセージ*で定義される管理者情報ラベル（デフォルト: *キャッシュ管理者:*）

<?error?>:ログイン試行中に発生するエラーメッセージ。

- すべてのホットスポットタイプで使用される変数

  <?terms?>:利用規約（*ホットスポット*ページでの定義）

  <?redirect_host?>:ホットスポットに対して指定されるリダイレクトURL（*ホットスポット*ページでの定義）

  <?location?>:ユーザが要求したURL

  <?location_host?>:ユーザが要求したURLのホスト名

  <?login_form?>:各ホットスポットタイプに適したログインフォーム: *パスワード*テキストボックス、*トークン*テキストボックス、*ユーザ名*および*パスワード*テキストボックス、または*同意*チェックボックス、および*ログイン*ボタン。カスタマイズされたログインフォームの作成については、下のユーザ固有のログインフォームを参照してください。

  <?asset_path?>(カスタマイズモード*フル*の場合のみ重要):ホットスポット固有の画像やスタイルシートの保存用ディレクトリ（使用例:<img src="<?asset_path?>/logo.png">）

- バウチャータイプのホットスポットでのみ使用される変数

  <?maclimit?>このホットスポットで許可されるバウチャー当たりのデバイスの数（*ホットスポット*ページでの定義）

  <?numdevices?>:このバウチャーで使用されるデバイスの数

  <?timeend?>:有効期限の終わり（*バウチャー定義*ページでの定義）

  <?time_total?>:許可される合計時間割当て（*バウチャー定義*ページでの定義）

  <?time_used?>:使用した時間割当て（*バウチャー定義*ページでの定義）

  <?traffic_total?>:許可される合計データ量（*バウチャー定義*ページでの定義）

  <?traffic_used?>:使用したデータ量（*バウチャー定義*ページでの定義）

テンプレートは、下のようなセクションを構成するif変数を含むことができます。それぞれのセクションには、開始変数と終了変数があります。ifセクションの内容は、特定の条件下でのみ表示されます。

If セクション	意味
<?if_loggedin?> <?if_loggedin_end?>	ユーザが正常にログインできるとセクションが表示されます。
<?if_notloggedin?> <?if_notloggedin_end?>	ユーザがまだログインしていない場合にセクションが表示されます。例、利用規約の承諾や発生したエラーのため。
<?if_authtype_password?> <?if_authtype_password_end?>	ホットスポットのタイプが、*当日有効パスワード*である場合に、セクションが表示されます。
<?if_authtype_disclaimer?> <?if_authtype_disclaimer_end?>	ホットスポットのタイプが、*利用規約の許諾*である場合に、セクションが表示されます。
<?if_authtype_token?> <?if_authtype_token_end?>	ホットスポットのタイプが、*バウチャー*である場合に、セクションが表示されます。
<?if_authtype_backend?> <?if_authtype_backendtoken_end?>	ホットスポットのタイプが、*バックエンド認証*である場合に、セクションが表示されます。
<?if_location?> <?if_location_end?>	ユーザがリダイレクトされるとセクションが表示されます。
<?if_redirect_url?> <?if_redirect_url_end?>	*ログイン後にURLへリダイレクト*チェックボックスが有効であれば、セクションが表示されます。
<?if_not_redirect_url?> <?if_not_redirect_url_end?>	*ログイン後にURLへリダイレクト*チェックボックスが無効であれば、セクションが表示されます。
<?if_timelimit?> <?if_timelimit_end?>	バウチャーに対して有効期限が設定されると、セクションが表示されます。
<?if_trafficlimit?> <?if_trafficlimit_end?>	バウチャーに対してデータ量が設定されると、セクションが表示されます。

Ifセクション	意味
<?if_timequota?> <?if_timequota_end?>	バウチャーに対して時間割当てが設定されると、セクションが表示されます。
<?if_maclimit?> <?if_maclimit_end?>	*バウチャー当たりのデバイス*の値が指定されると、セクションが表示されます。
<?if_terms?> <?if_terms_end?>	利用規約が定義され、有効になると、セクションが表示されます。
<?if_error?> <?if_error_end?>	ログイン試行中にエラーが発生すると、セクションが表示されます。

ユーザ固有のログインフォーム

事前定義された`<?login_form?>`変数の代わりに、独自にログインフォームを作成したい場合は、以下を考慮してください:

- フォームを以下のタグで囲む:

```
<form action="?action=login" method="POST">…</form>
```

- 利用規約承諾ホットスポットの場合、「accept」という名前のチェックボックスを追加する:

```
<input type="checkbox" name="accept">
```

- 当日有効パスワードまたはバウチャーホットスポットの場合、「token」という名前のテキストボックスを追加する:

```
<input type="text" name="token">
```

- バックエンド認証ホットスポットの場合、「username」および「password」という名前のテキストボックスを追加する:

```
<input type="text" name="username">
<input type="password" name="password">
```

- フォームを送信する方法を追加する。例、ログインボタン:

```
<input type="submit" name="login" value="Login">
```

12.6.3 バウチャー定義

*ワイヤレスプロテクション > ホットスポット > バウチャー定義*タブでは、バウチャータイプのホットスポットの各種バウチャー定義を管理できます。

バウチャー定義を作成するには、次の手順に従います。

1. ***バウチャー定義の追加*をクリックします。**
   *バウチャー定義の追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前：このバウチャー定義を説明する名前を入力します。

   有効期限：この定義のバウチャーの有効期間を指定します。このカウントは初回ログイン時から始まります。必ずこの期限を設定することをお勧めします。

   注 – *有効期限*最大期間は2年です。

   時間割当て：ここでは、許可するオンライン時間を制限できます。この定義のバウチャーの期限が切れるまでの最大オンライン時間を指定します。このカウントはログイン時から始まり、ログアウト時に停止します。さらに、5分間にわたってアクティビティがない場合にカウントが停止します。

   注 – *時間割当て*の最大期間は2年です。

   データ量：ここでは、許可するデータ量を制限できます。このバウチャー定義で送信できる最大データ量を入力します。

   注 – *最大データ量*は100 GBです。

   コメント（オプション）：説明などの情報を追加します。

3. ***保存*をクリックします。**
   バウチャー定義が作成されます。バウチャータイプのホットスポットの作成時には、このバウチャー定義を選択できるようになります。

バウチャー定義を編集または削除するには、対応するボタンをクリックします。

12.6.4 詳細

バウチャー一般オプション

ここには、期限切れになったバウチャーをデータベースから削除するかどうか、削除する場合は何日後に削除するかを指定できます。ホットスポットのログには、引き続き削除されたバウチャーの情報が表示されます。

ログインページ証明書

HTTPS経由で確実にログインするため、ページログインの証明書を選択できます。*Webサーバプロテクション* > *証明書管理* > *証明書*ページで、新しい証明書を作成およびアップロードできます。ドロップダウンリストから必要な証明書を選択して、*適用*をクリックして有効化します。

ウォールドガーデン Walled Garden

パスワードやバウチャーコードを入力しなくても、すべてのユーザが常にアクセスできる特定のホストまたはネットワークを追加または選択します。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

13 Webサーバプロテクション

この章では、Webサーバを攻撃や悪意ある行為から保護するSophos UTMのWebアプリケーションファイアウォールを設定する方法を説明します。

この章には次のトピックが含まれます。

13.1 WAF

Webアプリケーションファイアウォール(WAF)、あるいはリバースプロキシ)を使用すると、Sophos UTMによってWebサーバをクロスサイトスクリプティング(XSS)、SQLインジェクション、ディレクトリトラバーサルなどの攻撃や悪意ある行為、あるいはその他の潜在的な攻撃から防御することができます。DNATルールを使用して「実際の」マシンに変換される外部アドレス(仮想サーバ)を定義することができます。ここで、様々なパターンと検出方法を使用して、サーバを保護することができます。簡単に言うと、UTMのこのエリアでは、Webサーバから送受信されるリクエストに、利用条件を適用することができます。また、複数のターゲットに対する負荷分散が可能です。

13.1.1 仮想Webサーバ

*WAF > 仮想Webサーバ*タブでは、仮想Webサーバを作成できます。これらのWebサーバは、UTMの一部として、インターネットとWebサーバの間のファイアウォールを構築します。そのため、このような介入をリバースプロキシとも呼びます。UTMは、Webサーバへのリクエストをピックアップし、バックエンドWebサーバを様々な攻撃から保護します。それぞれの仮想サーバーはバックエンドWebサーバにマッピングされており、どのような保護レベル。また、複数のバックエンドWebサーバを1つの仮想Webサーバー定義。これにより、バックエンドWebサーバのロードバランシングを実行できます。

仮想サーバを追加するには、次の手順に従います。

1. ***新規仮想Webサーバ*ボタンをクリックします。**
   *仮想Webサーバを追加*ダイアログボックスが開きます。

2. **次の設定を行います。**

名前：仮想Webサーバを説明する名前を入力します。

インタフェース：Webサーバに到達するために使用するインタフェースをドロップダウンリストから選択します。

> **注** – IPv4アドレスとIPv6リンクローカルアドレスがフロントエンドインタフェースとして定義されているインタフェースがある場合、仮想WebサーバはIPv4アドレスにのみ到達可能です。IPv6リンクローカルアドレスのみが定義されているインタフェースは、仮想Webサーバのフロントエンドインタフェースとして選択できません。

タイプ：クライアントと仮想Webサーバとの間の通信を*平文 HTTP* とするか*暗号化 HTTPS* するか、または*暗号化 HTTPS およびリダイレクト*するかを決定します。リバース認証を使用したい場合は、安全上の理由から*暗号化 HTTPS* を選択することを強く推奨いたします。*暗号化 HTTPS およびリダイレクト*が有効であれば、`https://`なしでURLを入力するユーザは、自動的に仮想Webサーバにリダイレクトされます。

ポート：仮想Webサーバに外部から到達可能なポート番号を入力します。デフォルトはポート80（*平文 (HTTP)*）とポート443（*暗号化 (HTTPS)*）です。

証明書（*暗号化 HTTPS のみ*）：ドロップダウンリストからWebサーバの証明書を選択します。証明書は事前にWebサーバで作成し、*証明書管理* > *証明書*タブでアップロードしておく必要があります。

ドメイン：このフィールドには、証明書の作成されるホスト名が表示されます。

ドメイン（SAN証明書のみ）：WAFは、SAN（Subject Alternative Name）証明書をサポートします。証明書でカバーされるすべてのホスト名がこのボックスにリストされます。続いて、ホスト名の前にあるチェックボックスにチェックを入れて、複数のホスト名を選択することができます。

ドメイン（*平文 HTTP のみ*、またはワイルドカード付き*暗号化 HTTPS* ）：Webサーバが責任を持つドメインをFQDNとして入力します（例、`shop.example.com`、またはアクションアイコンを使用してドメイン名のリストをインポートします）。ドメインのプレフィックスで、ワイルドカードとしてアスタリスク（*）を使用できます（例：`*.mydomain.com`）。ワイルドカードによるドメインは、フォールバック設定とみなされます：ワイルドカードのドメインエントリがある仮想Webサーバが使用できるのは、より具体的にドメイン名が指定されている仮想Webサーバが他にない場合だけです。例：クライアントの要求`a.b.c`は、`*.c`より先に`*.b.c`に、さらに先に`a.b.c`と一致します。

バックエンド**Web**サーバ:新規バックエンドWebサーバを作成するか、ファイアウォールプロファイルを適用するWebサーバの前にあるチェックボックスにチェックを入れます。ミラーリングWebサーバがある場合、複数のWebサーバを選択することもできます。デフォルトでは、選択したWebサーバ間でトラフィックのロードバランシングが行われます。実装された要求カウントアルゴリズムは、それぞれの新しい要求を、その時点で最も小さい番号のアクティブな要求を持つWebサーバに割り当てます。*サイトパスルーティング*タブでは、詳細な負荷分散ルールを指定できます。

ファイアウォールプロファイル:ドロップダウンリストからファイアウォールプロファイルを選択します。このプロファイルは、選択したWebサーバを保護するために適用されます。また、ファイアウォールプロファイルを一切使用しない場合は*プロファイルなし*を選択できます。

コメント(オプション):説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**
圧縮サポートを無効にする(オプション):デフォルトでは、このチェックボックスは無効であり、クライアントがデータの圧縮を要求する場合、コンテンツは圧縮されて送信されます。圧縮によって転送速度が上昇し、ページの読み込み時間が短縮されます。ただし、Webサイトが適切に表示されない場合や、Webサイトへのアクセス中にコンテンツのエンコーディングエラーが発生する場合は、圧縮のサポートを無効にする必要があります。チェックボックスが有効であれば、WAFはこの仮想WebサーバのリアルWebサーバから圧縮されていないデータを要求し、HTTP要求のエンコーディングパラメータに関わらず、圧縮されていない状態でクライアントに送信します。

HTMLをリライト(オプション):このオプションを選択すると、返されたWebページのリンクUTMをが書き換えるため、リンクが有効に保たれます。例:バックエンドWebサーバのインスタンスの1つが、`yourcompany.local`というホスト名であるが、UTMでの仮想サーバのホスト名が`yourcompany.com`である。したがって、`<a href="http://yourcompany.local/">`のような絶対リンクは、クライアントへの配信前にリンクを`<a href="http://yourcompany.com/">`に書き換えなければ破損してしまいます。ただし、Webサーバで`yourcompany.com`が設定されているか、Webページの内部リンクが常に相対リンクとして表現されている場合には、このオプションを有効にする必要はありません。MicrosoftのOutlook Web AccessやSharepoint Portal Serverでは、このオプションを使用することを推奨します。

注 **–** 一部のリンクが正しく書き換えられず、無効となる場合もあります。リンクを一貫してフォーマットするよう、Webサイトの作者に依頼してください。

URL書き換えとは別に、HTML書き換え機能でも、正しくフォーマットされていないHTMLを次のように修正することができます。

- DOMツリーで、`<title>`タグを、ノード`html > title`から正しい`html > head > title`に移動する
- HTML属性値を囲む引用符を修正する(例:`name="value"`が`name="value"`になる)

注 – HTMLリライティングは、HTTPコンテンツタイプが`text/*`または`*xml*`(*はワイルドカード)のすべてのファイルに影響します。バイナリファイルなどの他のファイルタイプのHTTPコンテンツタイプが正しいことを確認してください。

クロスリファレンス – 詳しくは、libxmlドキュメントを参照してください(http://xmlsoft.org/html/libxml-HTMLparser.html)。

Cookieをリライト(オプション、*リライトHTML*が有効な場合のみ可視化):UTM返されたWebページのリライトCookieがある場合、このオプションを選択します。

注 – *リライトHTML*が無効の場合、*リライトCookie*も無効となります。

ホストヘッダをパス(オプション):このオプションを選択すると、クライアントに要求されたホストヘッダが保持され、Webリクエストとともに Webサーバへ転送されます。環境内で、ホストヘッダの受け渡しが必要かどうかは、Webサーバの設定に応じて決まります。

4. ***保存*をクリックします。**
   サーバが*仮想Webサーバ*リストに追加されます。

5. **仮想Webサーバを有効にします。**
   新しい仮想Webサーバは、デフォルトでは無効です(トグルスイッチはグレー)。仮想Webサーバを有効にするには、トグルスイッチをクリックします。

   これで仮想Webサーバが有効になります(トグルスイッチは緑)。

注 – 対応するインタフェースが無効である場合、仮想Webサーバの有効化はできません。インタフェースは、*インターフェース& ルーティング > インタフェース > インタフェース*で有効化できます。

*仮想Webサーバ*リストは、仮想Webサーバに割り当てられているそれぞれのリアルWebサーバのステータスアイコンを表示します。リアルWebサーバのステータスアイコンは、リアルWebサーバが有効でない場合は赤くなります。リアルWebサーバがダウンしているか利用できない場合はアンバー色、すべて正常に機能している場合は緑色です。

13.1.2 バックエンドWebサーバ

*WAF > バックエンドWebサーバ*タブで、WAFによって保護するWebサーバを追加できます。

Webサーバを追加するには、次の手順に従います。

1. ***新規バックエンドWebサーバ*ボタンをクリックします。**
   *リアルWebサーバを追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前：Webサーバを説明する名前を入力します。

   ホスト: ホストを追加または選択します。ホストは、タイプが*ホスト*または*DNSホスト*です。ここでは、DNSホスト名の使用を強く推奨します。これは、IPアドレスでリストされたホストは空のホストヘッダを送信するため、一部のブラウザで問題が発生するためです。定義を追加する方法は、*定義とユーザ > ネットワーク定義 > ネットワーク定義*ページで説明しています。

   タイプ: UTMとWebサーバの間の通信を*暗号化*するか、*平文*とするかを決定します。

   ポート: UTMとWebサーバの間の通信に使用するポート番号を入力します。デフォルトはポート80（*平文*）とポート443（*暗号化*）です。

   コメント（オプション）：説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**
   HTTPキープアライブを有効にする: デフォルトでは、WAFはHTTPキープアライブを使用します。つまり、HTTPの接続が永続し、これがCPUやメモリの使用を削減します。バックエンドWebサーバがHTTPキープアライブを適切にサポートしていない稀なケースでは、この機能により読み取りエラーやタイムアウトとなる可能性があるため、影響を受けるWebサーバに対して無効にする必要があります。仮想Webサーバに、HTTPキープアライブを無効にして、1つ以上のバックエンドWebサーバが割り当てられている場合、この仮想Webサーバに割り当てられているすべてのバックエンドWebサーバに対して機能が無効になります。

   タイムアウト: HTTPキープアライブのタイムアウト値をここに入力しす。入力できる値は、1～65535です。バックエンドがデータを送信している限り、タイムアウト期限となるまでは

データを受信可能です。期限後は、WAFがHTTP 502メッセージをクライアント宛てに送信します。デフォルトのタイムアウト時間は300秒です。

4. *保存*をクリックします。
サーバが*本Webサーバ*リストに追加されます。

*これで仮想Webサーバ*タブで存在するWebサーバをファイアウォールプロファイルに割り当てられるようになります。

13.1.3 ファイアウォールプロファイル

*WAF > ファイアウォールプロファイル*タブでは、Webサーバの保護モードとレベルを定義するWAFプロファイルを作成できます。

WAFプロファイルを作成するには、以下の手順に従います。

1. *新規ファイアウォールプロファイル*ボタンをクリックします。
*ファイアウォールプロファイルの追加*ダイアログボックスが開きます。

2. 次の設定を行います。
名前:プロファイルの名前を入力します。

Outlookはいつでも通過: WAF経由での外部Microsoft OutlookクライアントのMicrosoft Exchange Serverへのアクセスを許可します: Microsoft Outlookのトラフィックは、WAFによってチェックまたは保護されません。

モード:ドロップダウンリストからモードを選択します。

- モニタ: **HTTP**リクエストをモニタリングし、ログに記録します。
- リジェクト: HTTPリクエストは拒否されます。

選択したモードは、HTTPリクエストが下で選択したいずれかの条件と合致している場合に適用されます。

一般的脅威フィルタ: 有効にすると、複数の脅威からWebサーバを保護できます。下の*脅威フィルタカテゴリ*セクションで使用する脅威フィルタカテゴリを指定できます。すべてのリクエストは、選択したカテゴリのルールセットに対してチェックされます。結果に応じて、ライブログに通知や警告が表示されるか、直接リクエストがブロックされます。

厳密フィルタリング: 有効にすると、選択したルールのいくつかがより厳密になります。これは、誤検出につながることもあります。

フィルタルールのスキップ: 選択した脅威カテゴリに、誤検出につながるルールが含まれている場合もあります。特定のルールが原因である誤検出を回避するには、スキップしたいルールの番号をこのボックスに追加します。WAFルール番号は、*ログとレポート* > *Webサーバプロテクション* > *詳細*ページで、*上位ルール*フィルタを使用して取得できます。

Cookie署名: WebサーバをCookieの悪用から保護します。WebサーバがCookieをセットすると、最初のCookieに対して2つ目のCookieが追加されます。このCookieには、最初のCookieの名前、値、シークレットから構成されたハッシュが含まれており、シークレットはWAFによってのみ認識されます。したがって、要求によって正しいCookieペアが提供されない場合は、ある種の悪用が行われた可能性があり、Cookieは破棄されます。

*スタティック*URL強化: URL書き換えから保護します。そのため、クライアントがWebサイトを要求すると、そのWebサイトのすべてのスタティックURLに対して署名が行われます。この署名手順は、Cookie署名と似ています。さらに、次にどのリンクを有効に要求できるのかについて、Webサーバからの応答が解析されます。強化されたスタティックURLをブックマークし、後でアクセスすることができます。エントリURLを定義する方法を、以下のいずれかから選択します。

- *エントリ*URL*を手動で指定*: WebサイトのエントリURLとして機能するURLを入力します。これにより、署名が不要になります。以下の例の構文に準拠している必要があります。`http://shop.example.com/products/`、`https://shop.example.com/products/`あるいは`/products/`。
- *アップロードした*Google*サイトマップファイルからのエントリ*URL: ここで、Webサイトの構造に関する情報が含まれるサイトマップファイルをアップロードします。サイトマップファイルは、XML形式でもプレーンテキスト形式でもアップロードできます。後者のファイルはURLのリストのみが含まれます。プロファイルを保存すると、サイトマップファイルはWAFによって構文解析されます。
- **Google***サイトマップ*URL*からのエントリ*URL: UTMに、Webサイトの構造に関する情報が含まれるサイトマップファイルを、定義されたURLからダウンロードさせることができます。このファイルにアップデートがないか定期的にチェックすることができます。プロファイルを保存すると、サイトマップファイルはダウンロードされ、WAFによって構文解析されます。

  URL: サイトマップへのパスを絶対URLとして入力します。

  更新: ドロップダウンリストから更新間隔を選択します。*手動*を選択すると、サイトマップはこのプロファイルの更新を保存した場合にのみ更新されます。

> **注** – 指定のパスでフロントエンドモードの *フォーム*をともなうリバース認証を使用している場合、ログインフォームやこのパスに対し、エントリURLを指定する必要はありません。パスの設定方法は、*Webサーバプロテクション > WAF > サイトパスルーティング*ページに記載されています。

> **注** – URLハードニングは、HTTPコンテンツタイプが`text/*`または`*xml*`(*はワイルドカード)のすべてのファイルに影響します。バイナリファイルなどの他のファイルタイプのHTTPコンテンツタイプが正しいことを確認してください。コンテンツタイプが間違っていると、URLハードニング機能により破損する可能性があります。クライアントにより作成されたダイナミックURL(例:JavaScript)には有効でありません。

フォーム強化:URL書き換えから保護します。フォーム強化は、Webフォームのオリジナル構造を保持し、署名します。そのため、フォームの送信時にフォームの構造が変更されると、WAFは要求を拒否します。

> **注** – フォーム強化は、HTTPコンテンツタイプが`text/*`または`*xml*`(*はワイルドカード)のすべてのファイルに影響します。バイナリファイルなどの他のファイルタイプのHTTPコンテンツタイプが正しいことを確認してください。コンテンツタイプが間違っていると、ハードニング機能により破損する可能性があります。

ウイルス対策: このオプションを選択して、Webサーバをウイルスから防御します。

モード: Sophos UTMは、最高のセキュリティを実現するさまざまなウイルス対策エンジンを備えています。

- シングルスキャン: デフォルト設定。*システム設定 > スキャン設定*タブに定義されたエンジンを使用して最高レベルのパフォーマンスを実現します。
- デュアルスキャン: 各トラフィックに対し、異なるウイルススキャナを使用してスキャンを2回行うことにより、検知率を最大限に高めます。デュアルスキャンは、ベーシックガードサブスクリプションでは使用できません。

方向: ドロップダウンリストから、アップロードまたはダウンロードのいずれかをスキャンするか、その両方をスキャンするかを選択します。

スキャン不可 コンテンツをブロック: スキャンできないファイルをブロックするには、このオプションを選択します。スキャンできない理由はいくつかありますが、ファイルが暗号化されているか、破損している可能性があります。

スキャンサイズの制限：このオプションを選択すると、追加のフィールドにスキャンサイズの制限値を入力できます。制限値は単位メガバイトで入力します。

> 注 – スキャンサイズの制限は単一のファイルではなく1回のアップロードを参照します。例えば制限値を50MBにして、複数ファイルのアップロード（45MB、5MB、および10MB）を行うと、最後ファイルはスキャンされず、当該制限によりウィルスの検出が不可能となります。

> 注 – スキャンサイズの制限は単一のファイルではなく1回のアップロードを参照します。例えば制限値を50MBにして、複数ファイルのアップロード（45MB、5MB、および10MB）を行うと、最後ファイルはスキャンされず、当該制限によりウィルスの検出が不可能となります。

> 注 – 制限値を入力しない場合、「0」メガバイトとして保存され制限は無効となります。

評判の悪いクライアントをブロック: GeoIPおよびRBL情報に基づいて、評判の悪いクライアントを分類に従ってブロックすることができます。Sophosでは次の分類プロバイダを利用します。

RBLソース：

- Commtouch IP Reputation（ctipd.org）
- dnsbl.proxybl.org
- http.dnsbl.sorbs.net

GeoIPソースはMaxmindです。WAFは、次のいずれかのMaxmindカテゴリに属するクライアントをブロックします。

- A1：クライアントによって、IPアドレスや本来の所在地を隠すために使用される匿名プロキシまたはVPNサービス。
- A2：衛星プロバイダとは、衛星を利用して世界中の（多くの場合、高リスクな国の）ユーザにインターネットアクセスを提供しているISPです。

評判の悪いクライアントのリモートルックアップをスキップ: 評判ルックアップにはリモート分類プロバイダへの要求の送信が含まれるため、評判に基づくブロック機能を使用すると、システムのパフォーマンスが低下する可能性があります。このチェックボッ

クスは、GeoIPに基づく分類を使用する場合にのみ、チェックを入れてください。この場合、キャッシュされた情報を使用するため、パフォーマンスは大幅に向上します。

コメント(オプション):説明などの情報を追加します。

3. **オプションで、以下の脅威フィルタカテゴリを選択します。** *一般的脅威フィルタが有効な場合のみ使用可能* :

プロトコル違反:HTTPプロトコルのRFC標準仕様の遵守が強制されます。これらの標準への違反は、通常は悪意があります。

プロトコル異常:一般的使用パターンを検索。そうしたパターンがない場合、多くは悪意のリクエスト。こうしたパターンには、他のこと、「Host」や「User-Agent」などのHTTPヘッダも含まれます。

リクエスト制限:リクエスト引数の量と範囲に妥当な制限を強制する。リクエスト引数による過負荷は、典型的な攻撃ベクトルです。

HTTPポリシ:HTTPプロトコルの許可される使用を制限する。Webブラウザは、通常、すべての可能なHTTPオプションのうち、限られたサブセットだけを使用します。稀にしか使用しないオプションを許可しないことで、こうしたあまりサポートされていないオプションでの攻撃者の意図を防げます。

不良ロボット**(Bad Robots)**:ロボットやクローラの使用パターンの特性をチェックします。それらのアクセスを拒否することで、Webサーバで可能性がある脆弱性が露見しにくくなります。

ジェネリック攻撃 **(Generic Attacks)**:大半の攻撃に共通するコマンド実行の試みを検索する。Webサーバを破った後、攻撃者は通常、権限の拡大やデータ保存の操作などのサーバでのコマンドの実行を試みます。そうした違反実行の試みの形跡を検索することで、攻撃者は正当なアクセスによって脆弱なサービスをターゲットとするため、他の方法ではなかなか見つからない攻撃を検出できます。

SQLインジェクション攻撃:埋め込み**SQL**コマンドやリクエスト引数にあるエスケープ文字をチェックします。Webサーバでの攻撃の大半は、埋め込みSQLコマンドをデータベースに指示するために使用される入力フィールドをターゲットとしています。

XSS 攻撃:埋め込みスクリプトのタグやリクエスト引数のコードをチェックします。一般的なクロスサイトスクリプティン攻撃は、多くの場合合法な方法で、ターゲットとするWebサーバの入力フィールドへスクリプトコードを送り込むことを狙っています。

厳密なセキュリティ**(Tight Security)**:禁止されているパストラバーサルの試みをチェックするなど、リクエストに関して厳密なセキュリティチェックを実行します。

トロイの木馬：トロイの木馬の使用パターンの特性をチェックするために、トロイの木馬の活動を示すリクエストを検索します。ただし、見つからなければ、これはウイルス対策スキャナによってカバーされているので、こうしたトロイの木馬のインストールを防ぎます。

送信：Webサーバからクライアントへの情報の漏えいを防ぎます。これには、機密情報の収集や、特定の脆弱性の検出のために攻撃者が使用できるサーバによって送信されたエラーメッセージが含まれます。

4. *保存*をクリックします。
新しいWAFプロファイルが *ファイアウォールプロファイル*リストに追加されます。

URLハードニングとフォームハードニングに関する追加情報

URL強化とフォーム強化の両方を有効化することを推奨します。これら2つの機能は相補的なので、いずれか一方だけ有効化した場合に起こり得る問題を解決することができます。

- フォームハードニングだけ有効化した場合：Webページに、http://example.com/?view=article&id=1のように、クエリが追加されたハイパーリンクが含まれる場合（特定のCMSなど）、このようなページ要求はフォームハードニングによってブロックされます。これは、必要な署名が存在しないためです。
- URLハードニングだけ有効化した場合：WebブラウザがフォームデータをWebフォームのformタグのアクションURLに追加する場合（GET要求など）、フォームデータはWebサーバに送信される要求URLの一部となり、URL署名が無効になります。

両方の機能を有効化することで問題が解決するのは、フォーム強化とURL強化のいずれかが要求を有効だとみなすと、WAFが要求を受け付けるためです。

Outlook Web Access

Outlook Web Access（OWA）用のWAFの構成はややリスクを伴います。これは、OWAがパブリックIPからの要求を、内部LAN IPからのOWA Webサイトへの要求とは別の方法で処理するためです。OWAのURLにはリダイレクトが追加されます。外部アクセスのためには外部FQDNが使用されますが、内部要求には内部サーバのIPアドレスが使用されます。通知を表示するには、以下の設定を行う必要があります。

解決策は、OWA WebサーバのWAFプロファイルで、OWAディレクトリを*エントリURL*として設定することです（例：`http://webserver/owa/`）。さらに、パス`/owa/*`、`/OWA/*`のURLハードニングをスキップする除外を作成し、Cookie署名を仮想サーバに対して完全に無効化する必要があります。

ウイルス対策チェックをスキップする2番目の除外を作成し、`/owa/ev.owa*`パスの全カテゴリをスキップし、*URL強化またはフォーム強化実行時にHTMLを変更しない*高度機能を有効化します。

13.1.4 除外

WAF > *除外*タブでは、特定のチェックから除外されるWebリクエストや送信元ネットワークを定義できます。

1. ***除外*タブで、*新規除外リスト*をクリックします。**
   *除外リストを追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:除外を説明する名前を入力します。

   実行しないチェック:スキップするセキュリティチェックを選択します。説明は、*ファイアウォールプロファイル*を参照してください。

   スキップするカテゴリ:スキップする脅威フィルタカテゴリを選択します。説明は、*ファイアウォールプロファイル*を参照してください。

   仮想**Web**サーバ:選択されたチェックから除外する仮想Webサーバを選択します。

   全リクエストに適用:ドロップダウンリストから要求定義を選択します。ANDまたはORを使用して、2つの要求の定義を論理的に組み合わせることができます。

   ネットワーク:クライアント要求の発信元であり、選択されたチェックから除外する送信元ネットワークを追加または選択します。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

   パス:選択したチェックの免除の対象となるパスを追加します。完全なパスを入力(例:`/products/machines/images/machine1.jpg`など)、またはワイルドカードとしてアスタリスクを使用(例:`/products/*/images/*`)できます。

   コメント(オプション):説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**
   URL/フォームハードニング実行時に**HTML**を変更しない:選択すると、定義した除外設定と一致するデータがWAFエンジンにより変更されません。このオプションを使用すると、本Webサーバにより正しくないテキスト/HTMLコンテンツが提供されたバイナリデータが破損することがありません。その一方で、有効化されたURLハードニング、HTMLリライティング、またはフォームハードニングによってWebリクエストがブロックされることがあります。これらの3つの機能はHTMLパーサを使用するため、ある程度Webページコンテンツの変更に依存します。望ましくないブロックを回避するには、ブロックの影響を受ける要求に対してURLハード

ニング/フォームハードニングをスキップします。この設定は、WebサーバやWebページの依存関係に応じて、別の除外か新しい除外で行うことが必要な場合があります。

強化されていないフォームデータを受け入れる: *フォーム強化*の除外の対象であったとしても、フォーム強化署名が見当たらない場合は、そのフォームデータが受け入れが不可となる可能性があります。このオプションを利用すると、強化されていないフォームデータが受け入れられるようになります。

4. ***保存*をクリックします。**
   新しい除外ルールが*除外*リストに表示されます。

5. **除外リストを有効にします。**
   新しい例外はデフォルトで無効になっています(トグルスイッチはグレー表示)。例外を有効にするには、トグルスイッチをクリックします。

   これで除外リストが有効になります(トグルスイッチは緑色)。

除外ルールを編集または削除するには、対応するボタンをクリックします。

13.1.5 サイトパスルーティング

*WAF > サイトパスルーティング*タブでは、外部から受信したリクエストを転送する本Webサーバを定義できます。たとえば、`/products`などの特定パスのすべてのURLを特定Webサーバに送信することを定義できます。また、特定のリクエストに複数のWebサーバを許可する一方で、これらのサーバ間でリクエストを分散するためのルールを追加することもできます。たとえば、セッションの有効期間を通して各セッションを1つのWebサーバに関連付けること(スティッキーセッション)を定義できます。これは、オンラインショップをホストしている場合に、ユーザがショッピングセッション中に使用するサーバを1台に固定するためなどに必要になります。さらに、すべてのリクエストを1台のWebサーバに送信して、他のサーバをバックアップとしてのみ使用するように設定することもできます。

各仮想Webサーバには、1つのデフォルトサイトパスルート(/のパス)が自動的に作成されます。UTMでは、最も妥当な方法でサイトパスルートを自動的に適用し、最も厳格なパス、つまり最長のパスから始めて、他の特定サイトパスルートが外部から受信したリクエストと一致しない場合にのみ使用されるデフォルトパスルートまで順に適用します。サイトパスルートリストの順序は重要ではありません。デフォルトルートが削除された場合など、受信したリクエストに一致するルートがない場合は、リクエストが拒否されます。

注 – *サイトパスルーティング*タブは、1つ以上のバックエンドWebサーバと1つ以上の仮想サーバが作成されている場合にのみアクセスできます。

サイトパスルートを作成するには、次の手順に従います。

1. *新規サイトパスルート*ボタンをクリックします。
   *サイトパスルートを追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前：サイトパスルートを説明する名前を入力します。

   仮想**Web**サーバ：受信トラフィックの元のターゲットホストを選択します。

   パス：`/products/`など、サイトパスルートを作成するパスを入力します。

   リバース認証：このサイトパスルートへのアクセスが許可されるユーザやグループで認証プロファイルを選択します。プロファイルが選択されていなければ、認証は不要です。

   警告 – プレーンテキストモードで実行している仮想Webサーバでリバース認証プロファイルを使用すると、ユーザの資格情報が露出します。続行すると、Webアプリケーションファイアウォールは安全でない方法でユーザの資格情報を送信します。

   警告 – フロントエンドモードが*フォーム*である認証プロファイルは、仮想Webサーバで一度しか展開できません。

   バックエンド**Web**サーバ：指定するパスに使用するバックエンドWebサーバの前にあるチェックボックスにチェックを入れます。選択されているWebサーバの順序は、*ホットスタンバイモードを有効にする*オプションにだけ関連します。ソートアイコンを使用すると、順序を変更できます。

   アクセスコントロール：選択すると、*仮想Webサーバ*の特定のクライアントネットワークを許可またはブロックできます。クライアントは、自身のIPが*許可ネットワーク*リストに載っている場合にのみ、アクセスを得ます。*拒否ネットワーク*リストに載っているIPはブロックされます。どちらのリストも空である場合、*仮想Webサーバ*にはどこからも接続できません。IP特定のネットワークのみをブロックしたい場合、*すべて*を許可して、*拒否ネットワーク*を選択または追加します。特定のネットワークのみを許可したい場合、*許可ネットワーク*を選択または追加して、*拒否ネットワーク*を空にします。

   許可ネットワーク：*仮想Webサーバ*への接続を行える許可ネットワークを選択または追加します。

   拒否ネットワーク：*仮想Webサーバ*への接続をブロックする拒否ネットワークを選択または追加します。

   コメント（オプション）：説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**
   スティッキーセッションCookieを有効にする: 各セッションを1つのリアルWebサーバに関連付ける場合に、このオプションを選択します。これを有効にするとcookieがユーザのブラウザに渡され、これによりこのブラウザからのすべての要求を同じバックエンドWebサーバにルーティングするようUTMに指示が出されます。サーバが使用できない場合は、cookieが更新されず、セッションは別のWebサーバに切り替わります。

   ホットスタンバイモードを有効にする: すべてのリクエストを最初に選択したバックエンドWebサーバに送信し、他のWebサーバをバックアップとしてのみ使用する場合は、このオプションを選択します。バックアップサーバは、メインサーバに障害が発生した場合にのみ使用されます。*スティッキーセッションcookieを有効にする*オプションを選択していない限り、メインサーバが復旧するとすぐにセッションはメインサーバに戻ります。

4. ***保存*をクリックします。**
   *サイトパスルート*が*サイトパスルート*リストに追加されます。

サイトパスルートを編集または削除するには、対応するボタンをクリックします。

13.1.6 詳細

*Web アプリケーションファイアウォール > 詳細*タブでは、cookieの署名とURLハードニングに使用するキーを定義できます。

Cookie署名

ここでは、Cookie署名用の署名キーとして使用できるカスタムのシークレットを入力できます。

スタティックURLハードニング

ここでは、URLハードニング用の署名キーとして使用されるカスタムのシークレットを入力できます。

フォームハードニング

ここでは、フォームハードニングトークンの暗号キーとして使用されるカスタムのシークレットを入力できます。シークレットは8文字以上にする必要があります。

13.2 リバース認証

*Web サーバプロテクション > リバース認証*ページでは、Webアプリケーションファイアウォールをどのように使用するかを指定して、認証を実際のWebサーバに任せるのではなく、直接ユーザを認証

します。認証プロファイルによって、リバース認証を使用して、特定の認証設定をそれぞれのサイトパスルータに割り当てることができます。

認証プロファイルは、基本的には2つの認証モードで指定されます。ユーザとWAFの間で使用される認証モードと、WAF と実際のWebサーバの間で使用される認証モードです。こうして、実際のWebサーバが認証をサポートしていなくても、WAF はユーザに認証を強制することができます。他方、リバース認証は、それぞれの仮想Webサーバに複数の実際のWebサーバが割り当てられていても、ユーザが一度だけ認証を受ければ済むようにします。他方、リバース認証は、それぞれの仮想Webサーバに複数の実際のWebサーバが割り当てられていても、ユーザが一度だけ認証を受ければ済むようにします。

ユーザ認証のフォームを使用して、会社に固有のフォームテンプレートを指定することができます。

13.2.1 プロファイル

Web サーバプロテクション > *リバース認証* > *プロファイル*タブでは、Webアプリケーションファイアウォールの認証プロファイルを指定します。プロファイルを使用すると、異なるユーザやユーザグループに異なる認証設定を割り当てることができます。認証プロファイルを指定すると、*Web アプリケーションファイアウォール* > *サイトパスルーティング*タブでサイトパスルートに割り当てることができます。

認証プロファイルを追加するには、次の手順に従います。

1. ***プロファイル*タブで、*新規認証プロファイル*をクリックします。**
   *認証プロファイルの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前 : プロファイルの名前を入力します。

   仮想 **Web** サーバ : 仮想Webサーバプロファイル設定を、ここで設定できます。

   モード : Webアプリケーションファイアウォールでユーザがどのように認証するかを選択します。

   基本 : ユーザは、ユーザ名とパスワードを入力して、HTTP基本認証で認証を行います。このモードでは資格情報が暗号化されないで送信されるので、HTTPSで使用する必要があります。また、このモードでは、セッションCookieは生成されず、専用ログアウトはできません。

   フォーム : ユーザが資格情報を入力すると、フォームが表示されます。このモードでは、セッションCookieが生成され、専用ログアウトが可能です。使用するフォームテンプレートは、*フォーム テンプレート*ドロップダウンリストで選択しま

す。デフォルトのフォームテンプレート以外に、リストは*フォームテンプレート*タブで指定したフォームも表示します。

フォームテンプレート: 認証時にユーザに表示するフォームテンプレートを選択します。フォームテンプレートは、*フォームテンプレート*ページで指定します。

基本プロンプト: レルムとは、ログインページについてオン追加情報を提供し、ユーザオリエンテーションのために使用される一意の文字列です。

注 – 次の文字は*基本プロンプト*で使用可能です: A–Z a–z 0–9 , ; . : – _ ' + =) (& % $! ^ <> | @

ユーザ/グループ: ユーザまたはユーザグループを選択するか、この認証プロファイルに割り当てる必要がある新しいユーザを追加します。このプロファイルをサイトパスルートに割り当てると、ユーザはこのプロファイルで指定されている認証設定でサイトパスにアクセスできるようになります。一般的に、これはバックエンドのユーザグループです。ユーザを追加する方法は、*定義とユーザ > ユーザとグループ > ユーザ*ページで説明しています。ユーザグループを追加する方法は、*定義とユーザ > ユーザとグループ > グループ*ページで説明しています。

注 – 場合により、資格情報を入力する際、ユーザはユーザプリンシパル名表記「user@domain」の使用が求められることがあります(例: Exchange ServerをActive Directoryサーバと組み合わせて使用する場合など)。ユーザプリンシパル名表記の使用方法は*定義とユーザ > 認証サービス > サーバ > Active Directory*ページに記載されています。

リアルWebサーバ: リアルWebサーバのプロファイル設定を、ここで設定できます。

モード: Webアプリケーションファイアウォールが、リアルWebサーバに対して、どのように認証を行うかを選択します。このモードは、リアルWebサーバの認証設定と一致しなければなりません。

基本: 認証はHTTP基本認証で行われ、ユーザ名とパスワードが提供されます。

なし: WAFと実際のWebサーバの間で、認証は行われません。リアルWebサーバが認証をサポートしていなくても、ユーザはフロントモードで認証を行うことができます。

ユーザ名 アフィックス: ユーザ名のアフィックスを選択します。*プレフィックス*、*サフィックス*または両方を選択できます。アフィックスは、ドメインおよびEメールアドレスを扱う場合に有用です。

プレフィックス: *ユーザ名*のプレフィックスを入力します。

サフィックス: *ユーザ名*のサフィックスを入力します。

> 注 – プレフィックスおよびサフィックスは、ユーザが自身のユーザ名を入力すると自動的に追加されます。ユーザがプレフィックスおよびサフィックスを入力すると、追加はされません。例:サフィックスが`@testdomain.de`であり、ユーザが彼のユーザ名`test.user`を入力すると、サフィックスが追加されます。`test.user@testdomain.de`と入力すると、サフィックスは無視されます。

基本ヘッダを削除:このオプションを選択すると、基本ヘッダがUTMからリアルWebサーバへと送信されなくなります。

ユーザセッション: ユーザセッションタイムアウト設定を、ここで設定可能です。

セッションタイムアウト: 仮想Webサーバ上で何もアクションが実行されなかった場合、再度ログインをする際のユーザ資格情報確認を行うユーザセッションのタイムアウトを有効にするには、このオプションを選択します。

間隔の制限:セッションタイムアウトの間隔を設定します。

セッションタイムアウトスコープ: スコープを*日数*、*時間*、または*分*で設定します。

セッションの有効期間:アクティビティの平均時間にかかわらず、ログイン状態の保持時間に対しハードリミットを有効にするには、このオプションを選択します。

間隔の制限:セッションの有効期間値の間隔を設定します。

セッションの有効期間のスコープ: スコープを*日数*、*時間*、または*分*で設定します。

コメント(オプション):説明などの情報を追加します。

3. ***保存*をクリックします。**
   新しいプロファイルが*プロファイル*リストに表示されます。

プロファイルを編集または削除するには、対応するボタンをクリックします。

リバース認証：ユーザ/グループ

ユーザが資格情報を入力するのに、`user@domain`のフォーマットを使用しなければならない場合があります。例：Exchange ServerをActive Directoryサーバと組み合わせて使用する場合など。この場合、追加ステップを行います。

1. **WebAdminメニューから、*定義とユーザ* > *認証サービス* > *サーバ*タブを開きます。**
   *サーバ*タブが表示されます。

2. ***サーバ*タブで、所望のActive Directoryサーバの*複製*ボタンをクリックします。**
   新しいサーバが作成されます。

3. ***バックエンド*フィールドを*LDAP*に変更します。**

4. ***ユーザ属性*フィールドを>に変更します。**

5. ***カスタム*フィールドに`userPrincipalname`と入力します。**

まだ存在していない場合、これにより、*Active Directoryユーザ*グループの代わりに使用しなければならない*LDAPユーザ*グループを設定します。

> 注 – `domain\user`形式はサポートされていません。代わりに`user@domain`形式を使用します。

13.2.2 フォームテンプレート

Webサーバプロテクション > *リバース認証* > *フォームテンプレート*タブでは、リバース認証のためにHTMLフォームをアップロードすることができます。フォームテンプレートは、フロントエンドモードを*フォーム*として、認証プロファイルへ割り当てることができます。認証プロファイルが割り当てられているサイトパスにユーザがアクセスしようとすると、それぞれのフォームが表示されます。

フォームテンプレートを追加するには、次の手順に従います。

1. ***フォームテンプレート*タブで*新規フォームテンプレート*をクリックします。**
   *フォームテンプレートの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前：フォームテンプレートを説明する名前を入力します。

   ファイル名：フォルダアイコンをクリックして、HTMLテンプレートを選択、アップロードします。

   イメージ/スタイルシート：選択したフォームテンプレートで使用されているイメージ、スタイルシート、Javascriptファイルを選択、アップロードします。

コメント(オプション):説明などの情報を追加します。

3. *保存*をクリックします。
新しいフォームテンプレートが *フォームテンプレート*リストに表示されます。

フォームテンプレートを編集または削除するには、対応するボタンをクリックします。

ログインフォームテンプレートでの変数の使用

- 必須:

  方式がPostに設定されており、アクションが`<?login_path?>`に設定されている`<form>`要素。例:`<form action="<?login_path?>" method="POST"> ... </form>`

  名前がhttpd_usernameに設定されている、上述フォーム内の`<input>`要素。例:`<input name="httpd_username" type="text">`

  名前がhttpd_passwordに設定されている、上述フォーム内の`<input>`要素。例:`<input name="httpd_password" type="password">`

  注 – 正確に解析できるよう、あらゆるフォームテンプレートがこれらの3つの条件を満たすことが不可欠です(実際、`<?login_path?>`のみが置き換え可能)。

- オプション:

  `<?assets_path?>`のすべてのオカレンスは、フォームテンプレートと共にアップロードされた全アセットを含むパスにより置き換えられます。これにより、スタイルシート、画像などを実際のフォームテンプレート外部に配置してよりクリーンなフォームテンプレートにすることができます。例:`<link rel="stylesheet" type="text/css" href="<?assets_path?>/stylesheet.css">`

  `<?company_text?>`および`<?admin_contact?>`のすべてのオカレンスは、*マネジメント* > *カスタマイズ*で定義されるメッセージにより置き換えられます。例:<p>問題または質問がございましたら、`<?admin_contact?>`までご連絡ください。</p>

  `<?company_logo?>`のすべてのオカレンスは、*マネジメント* > *カスタマイズ*にアップロードされた画像へのパスに置き換えられます。例:`<img src="<?company_logo?>" alt="">`

9.2リリース以後、Sophos UTMにはデフォルトのフォームテンプレートが同梱されており、初期のリバース認証設定および導入が容易になりました。これは、デフォルトのフォームテンプレートに含まれているフォームです。

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
"http://www.w3.org/TR/html4/strict.dtd">
<html>

<head>
<link rel="stylesheet" type="text/css" href="<?assets_path?>/default_
stylesheet.css">
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
<title>ログイン</title>
</head>

<body>
<div id="container">

<div class="info"><img src="<?company_logo?>" alt=""><p><?company_
text?></p></div>

<form action="<?login_path?>" method="POST"><p><label for="httpd_
username">ユーザ名：</label><input name="httpd_username"
type="text"></p><p><label for="httpd_password">パスワード:</label><input
name="httpd_password" type="password"></p><p><input type="submit"
value="Login"></p></form>

<div class="note">トラブルやご質問がある場合は、こちらにご連絡ください
<b><?admin_contact?></b>.</div>

</div>
</body>

</html>
```

13.3 証明書管理

*Webサーバプロテクション > 証明書管理*メニューと*サイト間VPN > 証明書管理*メニューには、同じ設定オプションが含まれています。これらの設定オプションを使用すると、のすべての証明書関連オプションを管理することができます。Sophos UTM 中でも、X.509証明書の作成またはインポートや、*証明書失効リスト*(CRL)のアップロードなどを行うことができます。

13.3.1 証明書

*サイト間VPN > 証明書管理 > 証明書*を参照してください。

13.3.2 認証局 (CA)

*サイト間VPN > 証明書管理 > 認証局*を参照してください。

13.3.3 証明書失効リスト(CRL)

*サイト間VPN > 証明書管理 > 証明書失効リスト(CRL)*を参照してください。

13.3.4 詳細

*サイト間VPN > 証明書管理 > 詳細*を参照してください。

14 REDマネジメント

この章では、Sophos REDの設定方法について説明します。REDは*リモートイーサネットデバイス*の略で、リモートオフィス(遠隔地の支店)などを、あたかもローカルネットワークの一部であるかのようにメインオフィス(本社)に接続する手段です。

セットアップは、メインオフィスのSophos UTMとリモートオフィスのリモートイーサネットデバイス(RED)で構成されます。REDアプライアンス自体は設定する必要がないため、2拠点間の接続は非常に簡単に確立できます。REDアプライアンスは、UTMに接続するとただちに、UTM上の他のイーサネットデバイスと同じように動作します。支店のすべてのトラフィックはを介して安全にUTMルーティングされるため、支店はローカルネットワークと同じように安全になります。

現在使用できるRED アプライアンスは、次の2種類があります。

- RED 10:小さなリモートオフィス向けREDソリューション
- RED 50:アップリンクインタフェースが2つあるような、より大きなリモートオフィス向けREDソリューショ

この章には次のトピックが含まれます。

- 概要
- グローバル設定
- クライアントマネジメント
- 導入ヘルパ
- トンネルマネジメント
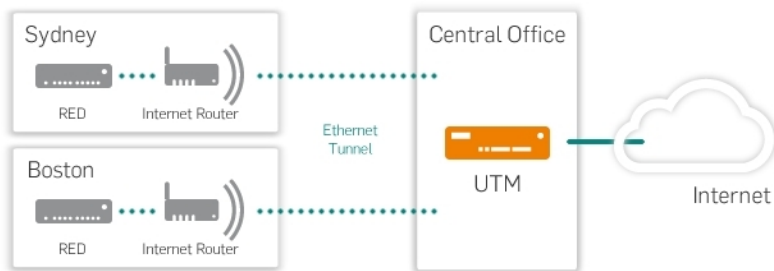
図 **24** RED:セットアップの略図

RED環境のセットアップは、以下の手順で行います。

1. REDサポートをアクティブにします。
2. UTM上でREDアプライアンスを設定します。
3. REDアプライアンスをリモートサイト上のインターネットに接続します。

注 – REDアプライアンスが設定されていないと、REDの概要ページには、REDアーキテクチャの一般的な情報が表示されます。REDアプライアンスを設定すると、そのページにはREDのステータスに関する情報が表示されます。

14.1 概要

*概要*ページは、REDの概要、その機能、および一般的なREDのセットアップについて基本情報を示します。

クロスリファレンス – REDデバイスの詳細情報は、*リソースセンター*にある*クイックスタートガイド*およびSophos UTM取扱説明書を参照してください。RED 10アプライアンスのLED 点滅コードは、SophosKnowledgebaseに説明があります。

RED ライブログを開く

ライブログを使用して、Sophos UTMとREDアプライアンスの間の接続をモニタリングすることができます。*RED ライブログを開く*ボタンをクリックすると、新しいウィンドウでライブログを開きます。

14.2 グローバル設定

*グローバル設定*タブでは、REDのサポートを有効または無効にすることができます。REDのサポートを有効にすると、UTMがREDハブとして機能します。REDサポートは、REDアプライアンスをUTMに接続する前に有効にしておく必要があります。

RED設定

REDサポートを有効にするには、次の手順に従います。

1. ***グローバル設定*タブで、REDサポートを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、*RED設定*エリアが編集可能になります。

2. **組織の詳細を入力します。**

デフォルトで、*マネジメント* > *システム設定* > *組織*タブの設定が使用されます。

3. ***REDの有効化*をクリックします。**
トグルスイッチが緑色になり、REDサポートが有効になります。これでUTMがのSophosRED プロビジョニングサービス(RPS)に登録され、REDハブとして機能するようになります。

これで、複数のREDアプライアンスを*クライアントマネジメント*ページに追加するか、*導入ヘルパページでウィザードを使用して継続することができます。*

設定をキャンセルするには、アンバー色のトグルスイッチをクリックします。

デバイスの自動認証解除

REDサポートが有効であれば、一定の時間間隔の後に、切断されたREDアプライアンスを自動的に認証解除するように指定できます。この機能により、盗難に遭ったREDアプライアンスがUTMに接続できないようにします。

注 –*デバイスの自動認証解除*は、2つのUTM間のREDトンネルには機能しません。

1. **自動認証解除を有効にします。**
*デバイスの自動認証解除を有効にする*チェックボックスを選択します。

2. **REDアプライアンスが自動認証解除までの時間間隔を指定します。**
必要な値を*認証解除までの時間*テキストボックスに入力します。最小時間間隔は5分です。

3. ***適用*をクリックします。**
これで、自動デバイス認証解除が有効になります。

定義された時間間隔より長い間切断されていた後に、REDアプライアンスが再接続すると、自動的に無効になります。これは、*クライアントマネジメント*ページのトグルスイッチで示されます。それぞれの警告も、同様に*概要*ページに表示されます。認証解除されたREアプライアンスの再接続を許可するには、*クライアントマネジメント*ページでREアプライアンスを有効にします。

REDの無効化

REDを無効にしても、REDは削除されません。RED機能を無効にすると、REDデバイスが無効化されその接続が失われます。UTMのRED機能を再度有効化すると、そのREDは再び有効となります。

REDを無効化するには、*グローバル設定*ページのトグルスイッチをクリックして、*RED設定の削除を確認*ボタンをクリックして確認します。

14.3 クライアントマネジメント

*REDマネジメント > クライアントマネジメント*ページでは、REDトンネルを使用してUTMに接続するために、リモートUTMを有効化することができます。これによりリモートUTMはREDアプライアンスのように機能するようになります。さらにここでは、導入ヘルパを使用する代わりに、REDアプライアンスを手動で設定することができます(エキスパートモード)。導入ヘルパは、REDアプライアンスの設定に使用できるより便利な機能で、次のWebAdminページに提供されています。

ここで設定した各REDアプライアンスまたはUTMは、UTMとの接続を確立できるようになります。

ページ名の前に*[サーバ]*タグが付いている場合は、UTMをサーバ(REDハブ)として機能させる場合にのみ、このページの設定が必要になることを表しています。

注 – REDアプライアンスの接続を可能にするためには、まず*グローバル設定*ページでREDサポートを有効にする必要があります。

2台のUTM間でのREDトンネルのセットアップ

REDトンネルを使用してローカルUTMに接続するために別のUTMを有効にするには、次の手順に従います。

1. ***クライアントマネジメント*タブで、*REDの追加*をクリックします。**
   *REDの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   ブランチ名:クライアントUTMが配置されたブランチ名を入力します(例:「ミュンヘンオフィス」)。

   クライアントタイプ: ドロップダウンリストから*UTM*を選択します。

   *トンネル***ID**: デフォルトでは*自動*が選択されています。トンネルには順番に番号が付けられます。両方のUTMのトンネルIDが一意であることを確認する必要があります。重複する場合は、ドロップダウンリストから別のIDを選択す必要があります。

   コメント(オプション):説明などの情報を追加します。

3. ***保存*をクリックします。**
   UTMオブジェクトが生成されます。

4. **プロビジョニングファイルをダウンロードします。**

リモート(クライアント)UTMに設定データを送るには、*ダウンロードUTM*ボタンを使用してプロビジョニングファイルをダウンロードし、安全な手段でリモートにファイルを送信します。

REDアプライアンスの設定

ローカルUTMに接続するためにREDアプライアンスを有効にするには、次の手順に従います。

1. ***クライアントマネジメント*タブで、*REDの追加*をクリックします。**
   *REDの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   ブランチ名:REDアプライアンスが配置されたブランチ名を入力します(例:「ミュンヘンオフィス」)。

   クライアントタイプ:接続しようとしているREDアプライアンスのタイプに応じて、ドロップダウンリストから*RED 10*または*RED 50*を選択します。

   > 注 – RED 50アプライアンスにはLCDディスプレイがあります。デバイスに関する重要な情報を表示するために使用できます。左ボタンで、メニューに入れます。アップおよびダウンボタンでナビゲートし、右ボタンで入ります。詳細情報は、取扱説明書を参照してください。

   RED ID:設定しているREDアプライアンスのIDを入力します。このIDは、REDアプライアンスの背面とパッケージに記載されています。

   トンネル**ID**:デフォルトでは*自動*が選択されています。トンネルには順番に番号が付けられます。IDが重複する場合は、ドロップダウンリストから別のIDを選択します。

   ロック解除コード(オプション):REDアプライアンスを初めて導入する場合は、このボックスは空白のままにします。設定中のREDアプライアンスを以前に導入したことがある場合は、ロック解除コードを指定する必要があります。ロック解除コードはREDアプライアンスの導入時に生成され、直ちに*グローバル設定*タブで指定したアドレスへメールが送信されます。これはセキュリティ機能であり、REDアプライアンスを簡単に切断してどこにでもインストールできなくなります。

   > 注 – USBスティックによる手動導入やRED Provisioning Service(下記参照)による自動導入では、2つの別個のロック解除コードが生成されます。ある導入方法から別の方法へREDデバイスを切り替える場合は、対応するロック解除コードを使用していることを確認し

てください:手動導入では、最後の手動導入でのロック解除コードを入力し、自動導入では、最後の自動導入でのロック解除コードを入力します。

ロック解除コードを紛失した場合、REDアプライアンスをロック解除するには、Sophosサポートに連絡してください。ただし、サポートが支援できるのは、SophosRED Provisioning Serviceによって自動的に構成を導入した場合だけです。

ヒント – ロック解除コードは、バックアップがホスト固有データを含んでいる場合にUTMREDのバックアップファイルで見つかることもあります。

UTMホスト名 : UTMがアクセスできるパブリックIPアドレスまたはホスト名を入力する必要があります。

第**2UTM**ホスト名 : RED 50アプライアンスでは、同じUTMの別のパブリックIPアドレスまたはホスト名を入力することもできます。別のUTMのIPやホスト名を入力することはできません。

第**2**ホスト名 の用途 (RED 50の場合のみ、下図参照):第二ホスト名を使用する対象を設定できます。

- フェイルオーバ: 第一ホスト名が失敗した場合に第二ホスト名を使用する場合にのみ選択します。
- バランス調整 : 両方のホスト名の間でアクティブ負荷分散を有効にする場合に選択します。これが意味を持つのは、第一ホスト名と第二ホスト名の両方のアップリンクに関連があり、レイテンシとスループットが等しい場合です。

アップリンクモード/**2**つ目 のアップリンクモード: REDアプライアンスのIPアドレスの取得方法は、DHCP経由またはスタティックIPアドレスの直接割り当てのいずれかで定義することができます。RED 50アプライアンスの場合、それぞれのREDアップリンクのイーサネットポートを別個に定義します。

- **DHCP**クライアント: REDはDHCPサーバからIPアドレスを取得します。
- スタティックアドレス: IPv4アドレス、対応するネットマスク、デフォルトゲートウェイ、DNSサーバを入力します。

注 –UTM ホスト名とREDアップリンクのイーサネットポートの間には1対1の関係はありません。それぞれのREDポートは、UTMそれぞれ定義済みのホスト名と接続しようとします。

第二アップリンクの使用対象(RED 50の場合のみ、下図参照):第二アップリンクを使用する対象を設定できます。

- フェイルオーバ:第一アップリンクが失敗した場合に第二アップリンクを使用する場合にのみ選択します。
- バランス調整:両方のアップリンクの間でアクティブ負荷分散を有効にする場合に選択します。これが意味を持つのは、RED 50アプライアンスの両方のアップリンクのレイテンシとスループットが等しい場合です。

オペレーションモード:リモートネットワークのローカルネットワークへの統合方法を定義できます。

- 標準/統合:UTMがリモートネットワークのネットワークトラフィックを完全にコントロールします。さらに、DHCPサーバおよびデフォルトゲートウェイとして機能します。すべてのリモートネットワークはUTM経由でルーティングされます。
- 標準/分割:UTMがリモートネットワークのネットワークトラフィックを完全にコントロールします。さらに、DHCPサーバおよびデフォルトゲートウェイとして機能します。統合モードと違い、特定のトラフィックのみがUTM経由でルーティングされます。下の*分割ネットワーク*ボックスに、リモートクライアントからアクセス可能なローカルネットワークを定義します。

  注 – VLANタグの付いたフレームは、この操作モードでは処理できません。REDアプライアンスの背後でVLANを使用している場合合は、代わりに*標準*モードを使用してください。

- 透過/分割:UTMは、リモートネットワークのネットワークトラフィックをコントロールせず、DHCPとしてもデフォルトゲートウェイとしても機能しません。代わりに、リモートネットワークのDHCPサーバからIPアドレスを取得して、ネットワークの一部とします。ただし、リモートクライアントからローカルネットワークへのアクセスは有効にすることができます。そのために、リモートネットワークによるアクセスを許可する*分割ネットワーク*を定義する必要があります。さらに、1つ以上の*分割ドメイン*をアクセス可能として定義することができます。ローカルドメインがパブリックに解決可能ではない場合、リモートクライアントからクエリ(問い合わせ)可能な*分割DNSサーバ*を定義する必要があります。

> 注 – VLAN タグの付いたフレームは、この操作モードでは処理できません。RED アプライアンスの背後で VLAN を使用している場合合は、代わりに*標準*モードを使用してください。

すべてのオペレーションモードの例は、*導入ヘルパ*タブで参照できます。

3. **RED 50では、オプションで、以下のスイッチポートを設定できます**:
   LAN ポートモード: RED 50には、シンプルなスイッチまたはインテリジェントなVLAN使用のどちらかとして設定できるLANポートが4つあります。*スイッチ*に設定すると、基本的にすべてのトラフィックがすべてのポートに送信されます。これに対して、*VLAN*に設定した場合、イーサネットのフレームのVLANタグに従ってトラフィックをフィルタすることができるので、複数のネットワークをREDトンネルでトンネル化することができます。

   LAN モード: VLANスイッチポートの構成で使用する場合、それぞれのLANポートを個別に設定することができます。それぞれのLANポートに対して、次の設定を使用できます。

   タグなし: 下の*LAN VID*フィールドでVLAN IDが指定されたイーサネットのフレームがこのポートに送信されます。フレームがタグなしで送信されるので、エンドデバイスはVLANをサポートしません。このポートで許可されるVLAN IDは1つだけです。
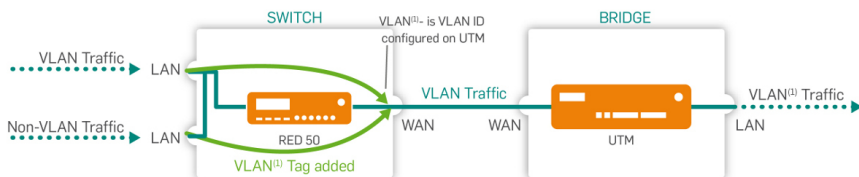
図 **25** LANモード:タグなし

   タグなし,、ドロップタグあり: 下の*LAN VID*フィールドでVLAN IDが指定されたイーサネットのフレームがこのポートに送信されません。フレームがタグなしで送信されるので、エンドデバイスはVLANをサポートしません。
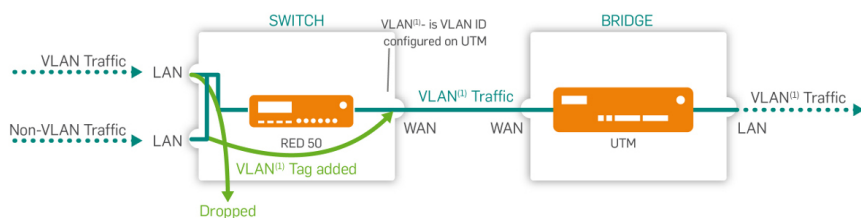
図26 LANモード:タグなし、ドロップタグあり

タグあり: 下の*LAN VID*フィールドでVLAN IDが指定されたイーサネットのフレームがこのポートに送信されます。フレームがタグ付きで送信されるので、エンドデバイスはVLANをサポートします。VLAN IDが指定されていないフレームは、このポートに送信されません。このポートでは、最大で64までのコンマで区切られたVLAN IDが許可されます。
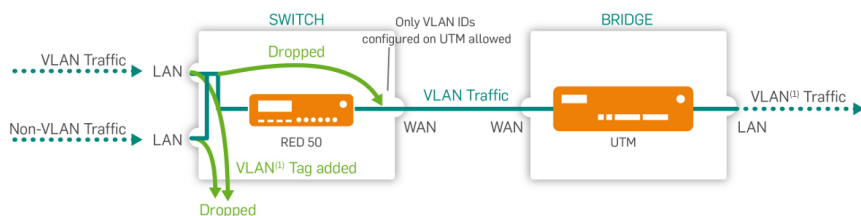
図27 LANモード:タグあり

無効:このポートは閉じています。*LAN VID*フィールドでのVLAN IDの指定に関わらず、フレームはこのポートに送信されます。
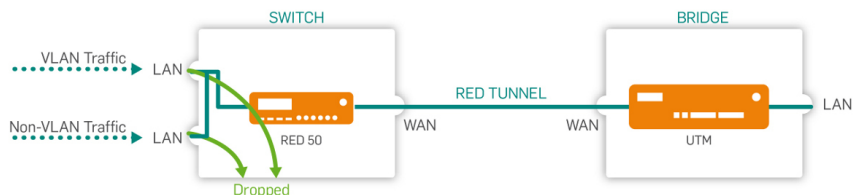
図28 LANモード:無効

> 注 – *LAN モード*には、Cisco/HPドキュメントに別の名前があります。*タグなし*別名「ハイブリッドポート」、*タグなし、ドロップタグあり*別名「アクセスポート」および*タグあり*別名「トランクポート」。

コメント(オプション):説明などの情報を追加します。

4. **次の詳細設定を任意で行います。**
MAC *フィルタリングタイプ*: このワイヤレスネットワークにアクセスできるMACアドレスを制限するには、*ブラックリスト*または*ホワイトリスト*を選択します。*ブラックリスト*を使用する場合、以下の MAC アドレスリストで指定したものを除く、すべての MAC アドレスが許可されます。*ホワイトリスト*を使用する場合、以下の MAC アドレスリストで指定したものを除く、すべての MAC アドレスがブロックされます。

 MAC *アドレス*: ワイヤレスネットワークへのアクセスを制限するために使用される MAC アドレスのリスト。MACアドレスリストは、*定義とユーザ* > *ネットワーク定義* > *MAC アドレス定義*タブで作成できます。RED 10では最大200のMACアドレスが許可されますが、RED 50では、リストに最大400のMACアドレスを含めることができます。

> 注 – MACフィルタリングが機能するには、RED rev. 2以降だけです。

デバイス導入:REDの設定に必要な構成をどのように提供するかを選択します。デフォルトでは、UTMはREDの構成データをSophosRED Provisioning Serviceを通じて自動的に提供します。この場合、REDアプライアンスはその構成をインターネットを通じて受け取ります。たとえば、REDにインターネット接続がない場合は、USBスティックを使って、手動で構成を提供することができます。REDデバイスを手動で配備する場合、UTMがNTPサーバーとして機能していることを確認する必要があります。そのため、UTM上でNTPを有効にして、適正なネットワークを許可します。または、少なくともREDのIPアドレスを許可します。

> 注 –Sophos UTM バージョン9.2以前:REDを手動で配備後に、再度手動で配備する前に、RED Provisioning Service(自動)を使用して1回配備する必要があります。手動でのデバイス導入が機能できるのは、ファームウェアのバージョンが9.1またはそれ以降のREDアプライアンスだけです。

警告 – 手動導入を選択する場合、メールで送信されるロック解除コードを保持していることが極めて重要です。もしロック解除コードを失うと、REDアプライアンスを別のに接続することはUTM不可能になります。

データ圧縮:データ圧縮を有効にすると、REDトンネルを通して送信されるすべてのトラフィックを圧縮します。データ圧縮により、1～2 Mbpsなどの非常に遅いインターネット接続をともなうエリアのREDアプライアンスのスループットを増加させる場合があります。ただし、増加する任意のパフォーマンスは、主に送信するデータのエントロピーに依存します(例:HTTPSやSSHなど既に圧縮されたデータはこれ以上圧縮することはできません)。そのため状況により、データ圧縮の有効化により、REDアプライアンスのスループットが実際には軽減する可能性もあります。その場合、データ圧縮を無効にしてください。

注 – データ圧縮はRED 10 rev.1では使用することができません。

3G/UMTSフェイルオーバー: RED rev. 2から、REDアプライアンスがUSBポートを提供し、ここに3G/UMTS USBスティックをつなぐことができます。選択すると、WANインタフェースで障害が発生したときに、このスティックがインターネットのアップリンクフェイルオーバとして機能します。必要な設定については、インターネットプロバイダのデータシートを参照してください。

- ユーザ名/パスワード(オプション):必要な場合、モバイルネットワークのユーザ名とパスワードを入力します。
- **PIN**(オプション):PINが設定されている場合、SIMカードのPINを入力します。

注 – WANインターフェイスの障害の際に間違ったPINを入力すると、3G/UMTSによって接続を確立することはできません。代わりに、REDアプライアンスの*3G/UMTS フェイルオーバー*チェックボックスが自動的に選択解除されます。そのため、間違ったPINは一度しか使用されません。WANインターフェイスが再度起動されると、REDアプライアンスに次の警告が表示されます:*3G/UMTS フェイルオーバーアップリンクに間違ったPINが入力されました。ログインデータを変更してください。REDの編集*ダイアログボックスを開くと、*3G/UMTS フェイルオーバー*が自動的に選択解除されたことを知らせるメッセージが表示されます。PINを訂正してから、チェックボックスを再選択してください。間違ったPINで3回接続を試みると、SIMカードがロックされることに注意してください。REDアプライアンスやUTMでは、このロックを解除することはできません。サポートされている*3G/UMTS* USBスティックの大

半について、シグナル強度がライブログおよびRED 50 LCDディスプレイに表示されます。

- モバイルネットワーク:モバイルネットワークタイプをGSMまたはCDMAから選択します。
- **APN**:プロバイダのアクセスポイント名情報を入力します。
- ダイヤル文字列(オプション):プロバイダが異なるダイヤル文字列を使用している場合、ここに入力します。デフォルトは「*99#」です。

注 – 次の設定は必ず手動で行ってください。1)必要なファイアウォールルールの作成(*ネットワークプロテクション* > *ファイアウォール* > *ルール*)。2)必要なマスカレードルールの作成(*ネットワークプロテクション* > *NAT* > *マスカレード*)。

5. *保存***をクリックします。**
   REDアプライアンスが作成され、*RED*リストに表示されます。

自動デバイス導入では、REDのブート(起動)直後に、SophosRED Provisioning Service (RPS)から設定が取得されます。その後、UTMとREDアプライアンス間の接続が確立されます。

手動デバイス導入では、*RED*リストの新しいエントリに*ダウンロード*ボタンがあります。設定ファイルをダウンロードして、USBスティックのルートディレクトリに保存します。次に、USBスティックを、電源をオンにする前のREDアプライアンスにつなぎます。REDは、USBスティックから設定を取り込みます。その後、UTMとREDアプライアンス間の接続が確立されます。

警告 – *REDアプライアンスが設定を受信した直後に*グローバル設定タブで指定したアドレスにメールで送信されるロック解除コードを保持しておくことが重要です。(手動導入と自動導入を切り替える場合は、両方のロック解除コードを保持しておく必要があります。)REDアプライアンスを他のUTMと使用したい場合に、ロック解除コードが必要になります。ロック解除コードが手元にない場合、REDアプライアンスをロック解除するためには、Sophosサポートに連絡する必要があります。ただし、サポートが支援できるのは、SophosRED Provisioning Serviceによって自動的に構成を導入した場合だけです。

REDアプライアンスを編集するには、対応するボタンをクリックします。設定されたすべての*RED*アプライアンスのステータスは、WebAdminのRED概要ページで確認できます。

下の図は、RED 50が提供する4つのバランシング/フェイルオーバーの組み合わせの概要を示しています。実線がバランシングの動作を、破線がフェイルオーバの動作を示しています:
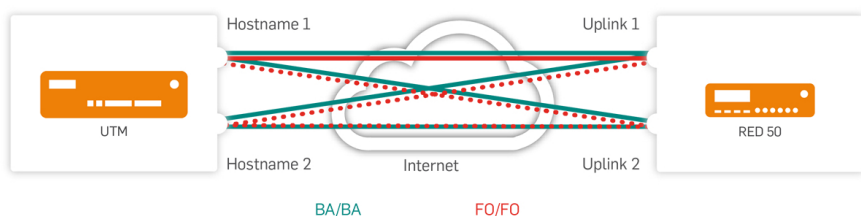
図 **29** RED 50:ホスト名とアップリンクバランス(ターコイズ色)およびホスト名とアップリンクフェイルオーバー(赤色)
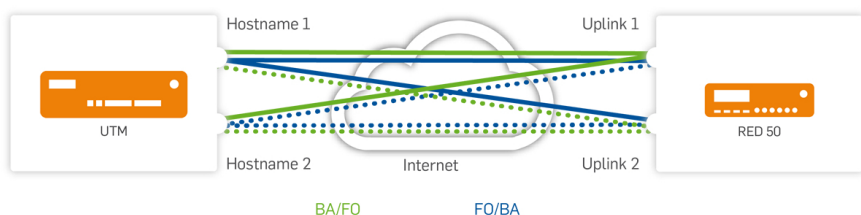
図 **30** RED 50:ホスト名とアップリンクフェイルオーバー(緑色)およびホスト名フェイルオーバーとアップリンクバランス(青色)

RED 50バランシングについての一般情報

バランシングアルゴリズムより、ソース基づく送信リンクおよび宛先IPアドレスが選択されます。パケットに基づいてバランシングされるのではありません。この理由は、単一TCP接続でパスが異なっていることが原因でパケットが並べ替えられる場合、TCPパフォーマンスに非常に負担がかかるからです

これは、同一ソースによる送信および宛先IPアドレスは常に、同じインタフェースの組み合わせとなることを意味します。例えば、UTM上ではWAN 1の送信パケットはuplink 1に対応し、UTM上のuplink 2からの受信パケットはWAN 1に対応します。RED 50の背後のクライアントが大きいファイルをダウンロードする場合、すべての受信パケットは1つのインタフェース経由でのみで送信されます。クライアントが2つのファイルを2つの異なるサーバからダウンロードする場合、受信パケットは、IPアドレスにより1つのインタフェースでまたは両方のインタフェースで送信されます。

バランシング設定は以下の通りです。

バランシング有 りのRED 50、UTMに1つのアップリンク付 き。

1. *UTMホスト名*のみを入力します。
2. バランシングの第一および第二のアップリンクを設定します。

> **注** – *第二のUTMホスト名*は入力しないでください。また、同じIPまたは名を2回入力しないでください。

バランシング有 のRED 50、バランシングモードでUTMに2つのアップリンク付 き。

1. UTMの2つの異なるホスト名およびのIPアドレスを入力します。
2. バランシングの第一および第二のアップリンクを設定します。
3. *インタフェース& ルーティング > アップリンクバランス*の2つのホスト名とIPアドレスについて、UTMアップリンクバランスが有効となっていることを確認してください。

RED 50に1アップリンク付 き、バランシングモードでUTMに2アップリンク付 き。

1. UTMの2つの異なるホスト名およびのIPアドレスを入力します。
2. *インタフェース& ルーティング > アップリンクバランス*の2つのホスト名とIPアドレスについて、UTMアップリンクバランスが有効となっていることを確認してください。

> **注** – アップリンクバランスが有効になっていないと、dmesg errorメッセージ「*IPv4: martian source...*」がUTM上に表示されます。

REDアプライアンスの削除

REDアプライアンスを削除するには、アプライアンス名の横にある*削除*ボタンをクリックします。

REDオブジェクトに依存関係があるという警告が表示されます。REDアプライアンスを削除しても、関連するインタフェースと依存関係は*削除されません*。これは、REDアプライアンス間でインタフェースを移動できるようにするための意図的な設計です。

REDアプライアンスの設定を完全に削除するには、潜在的なインタフェースとその他の定義を手動で削除してください。

14.4 導入ヘルパ

*REDマネジメント > 導入ヘルパ*タブには、RED環境のセットアップと統合のためのウィザードがあります。このウィザードは、*クライアントマネジメント*タブでの通常の設定の簡易版となります。必須フィールドと、必要に応じて*オプション*マークの付いたフィールドに入力して、*REDの導入*をクリックするだけです。

ページ名の前に*[サーバ]*タグが付いている場合は、UTMをサーバ（REDハブ）として機能させる場合にのみ、このページの設定が必要になることを表しています。

> 注 – 利便性のため、*標準*および*標準/分割*モードでは、*クライアントマネジメント*タブと違い、導入ヘルパが指定したIPアドレスのローカルインタフェース、利用可能なIPアドレス範囲の半分をカバーするリモートネットワーク用DHCPサーバー、ローカルDNSリゾルバへのアクセスといったオブジェクトを自動的に作成します。*透過/分割*モードでは、導入ヘルパはDHCPクライアント（*Ethernet DHCP*）インタフェースのみを作成します。

導入ヘルパは、各オプションについて概要を提供し、REDテクノロジーで提供される3つのオペレーションモードそれぞれについてスケッチを提供します。

以下は、REDの3つのオペレーションモードの説明と使用例です。

標準/統合

UTMがリモートネットワーク全体を管理します。DHCPサーバーおよびデフォルトゲートウェイとして機能します。

例：支店が1つあり、セキュリティ上の理由から、そのすべてのトラフィックを本店のUTM経由でルーティングしたい。これにより、リモートサイトは、LAN経由で接続されているようにローカルネットワークの一部となります。

標準/分割

> 注 – VLANタグの付いたフレームは、この操作モードでは処理できません。REDアプライアンスの背後でVLANを使用している場合合は、代わりに*標準*モードを使用してください。

*標準*モードと同様に、UTMがリモートネットワーク全体を管理します。DHCPサーバーおよびデフォルトゲートウェイとして機能します。ただし、*分割ネットワーク*ボックスにリストされたネットワーク宛てのトラフィックのみが、ローカルUTMにリダイレクトされる点が異なります。定義された分割ネットワークを宛先としていないすべてのトラフィックは、インターネットに直接ルーティングされます。

例：支店が1つあり、セキュリティ上の理由から、ローカルイントラネットへのアクセスを必要としているか、UTMリモートネットワークのトラフィックを経由でルーティングしたい（例えば、トラフィックに対するウイルスチェックのため、あるいはHTTPプロキシを使用するため）。

透過/分割

注 – VLAN タグの付いたフレームは、この操作モードでは処理できません。RED アプライアンスの背後で VLAN を使用している場合合は、代わりに*標準*モードを使用してください。

リモートネットワークは独立したままで、UTMはIPアドレスをリモートDHCPサーバーから取得してこのネットワークの一部となります。リモートネットワークの特定のトラフィックのみ、特定のネットワークまたはローカルドメインへのアクセスが許可されます。UTMはリモートネットワークをコントロールできないため、*分割DNSサーバー*を定義しない限り、パブリックに解決可能ではないローカルドメインをリモートルータで解決することはできません。これは、リモートクライアントからクエリ（問い合わせ）可能なローカルDNSサーバです。

技術的には、REDアプライアンスのローカルインタフェースと、ローカルのUTMへのアップリンクインタフェース、並びにリモートルータへのリンクは、このモードでブリッジされます。（RED 50アプライアンスでは、LANポートはWANにだけブリッジされます。）UTMがリモートネットワークの唯一のクライアントであるため、他のモードと同様に、分割ネットワークへのトラフィックのルーティングはできません。そのため、REDアプライアンスはすべてのトラフィックをインターセプトします。*分割ネットワーク*ボックスにリストされたネットワーク宛てのトラフィックや、*分割ドメイン*ボックスにリストされたドメイン宛てのトラフィックは、インタフェースUTMにリダイレクトされます。これは、各データパケット内でデフォルトゲートウェイのMACアドレスをUTMのMACアドレスに置き換えることで実現します。

例：イントラネットや、ローカルネットワーク内の特定のサーバへのアクセスが必要なパートナーまたはサービスプロバイダがいる。REDアプライアンスを使用することで、このパートナーのネットワークは自社のネットワークからの独立が完全に保たれますが、特定の目的のために、自社のネットワークの決められた部分にLAN経由で接続しているかのようにアクセスすることはできます。

注 –導入ヘルパを使用すると、REDアプライアンスのアップリンクモードはいずれのオペレーションモードでも*DHCPクライアント*となります。代わりにスタティックIPアドレスを割り当てる必要がある場合は、*クライアントマネジメント*タブでREDアプライアンスを設定する必要があります。

14.5 トンネルマネジメント

*REDマネジメント> トンネルマネジメント*ページでは、別のUTMにREDトンネルを確立するために、UTMをRED アプライアンスとして機能するように設定できます。これにより、リモートホストがのREDハブとして機能するようになります。これにより、リモートホストUTMがUTMのREDハブとして機能するようになります。

ページ名の前に*[クライアント]*タグが付いている場合は、UTMをREDクライアントとして機能させる場合にのみ、このページの設定が必要になることを表しています。

UTMをホストUTMに接続するためには、プロビジョニングファイルが必要になります。このファイルはホストUTMで作成する必要があります（*クライアントマネジメント*を参照）。

UTMをホストUTMに接続するには、次の手順に従います。

1. ホスト**UTM**で、ローカル**UTM**を*クライアントマネジメント*リストに追加します。
2. ホスト**UTM**で、**UTM**のプロビジョニングファイルをダウンロードします。
3. **ローカルUTMで** *トンネルを追加***をクリックします。**
   *トンネルの追加*ダイアログボックスが開きます。
4. **次の設定を行います。**
   トンネル名 : このトンネルを説明する名前を入力してください。

   UTMホスト: リモートUTMホストを選択します。

   Prov. ファイル : フォルダアイコンをクリックし、アップロードするプロビジョニングファイルを選択して、*アップロード開始*をクリックします。

   コメント(オプション) : 説明などの情報を追加します。
5. *保存***をクリックします。**
   REDトンネルが確立され、*トンネルマネジメント*リストに表示されます。

15 サイト間VPN

この章ではSophos UTMのサイト間 VPN 設定の構成方法について説明します。Sophos UTMのサイト間VPNは、*バーチャルプライベートネットワーク VPN* によって実現します。VPNはインターネットなどの公共のネットワーク上でリモートネットワークが極秘に相互通信するためのセキュアでコスト効果の高い方法です。VPNでは暗号化トンネリングプロトコルのIPsecを使用して、VPN上を伝送されるデータの機密性とプライバシを保ちます。VPN では暗号化トンネリングプロトコルの IPsec を使用して、VPN 上を伝送されるデータの機密性とプライバシーを保ちます。

> クロスリファレンス – サイト間VPN接続の設定方法の詳細は、SophosKnowledgebaseを参照してください。

この章には次のトピックが含まれます。

- Amazon VPC
- IPsec
- SSL
- 証明書管理

WebAdmin の *サイト間 VPN*概要ページには、設定されたすべての Amazon VPC、IPsec、および SSL コネクションとその現在のステータスが表示されます。各コネクションの状態は、そのステータスアイコンの色で示されます。ステータスアイコンは 2種類あります。コネクション名の隣りの大きなアイコンは、コネクションの全体的な状態を表します。それぞれの色は以下の状態を意味します。

- 緑色 – すべての SA (*セキュリティアソシエーション*) が確立されました。コネクションは完全に機能しています。
- 黄色 – SA の一部が確立されていません。コネクションは部分的に機能しています。
- 赤色 – SA がまったく確立されていません。コネクションが機能していません。

トンネル情報の隣りの小さなアイコンは、トンネルの状態を表します。それぞれの色は以下の状態を意味します。

- 緑色 – すべてのSA が確立されました。トンネルは完全に機能しています。
- 黄色 – IPsec SA が確立されましたが、ISAKMP SA (*インターネットセキュリティアソシエーションと鍵管理プロトコル*) が機能していません。トンネルは完全に機能しています。
- 赤色 – SA がまったく確立されていません。コネクションが機能していません。

15.1 Amazon VPC

Amazon VPC(バーチャルプライベートクラウド)は、商業的なクラウドコンピューティングサービスです。ユーザはバーチャルプライベートクラウドを作成した後、これをローカルネットワークに接続して、IPsecトンネルで集中管理することができます。

Sophos UTMにスタティックのパブリックIP アドレスがある場合は、Amazon VPCをUTMに接続できます。VPN接続のすべての設定は、Amazon 環境で行う必要があります。その後は、Amazonアクセスデータまたは設定ファイルを使用して接続データをインポートするだけで済みます。

15.1.1 ステータス

*サイト間VPN > Amazon VPC > ステータス*ページには、Amazon VPCのすべてのコネクションがリストされます。

ここでは、接続を有効または無効にすることができます。

Amazon VPCの接続を有効にするには、以下の手順に従います。

1. *セットアップ*ページで、**VPC接続を1つ以上インポートします。**

2. *ステータス*ページで、**Amazon VPCを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチが緑色になり、インポートされたVPC接続が表示されます。

3. **目的の接続を有効にします。**
   有効にするコネクションのトグルスイッチをクリックします。

   トグルスイッチが緑色になり、VPCコネクションの2つのトンネルが表示されます。

> 注 – 各接続は、冗長化のためにアクティブなトンネルとバックアップトンネルの2つのトンネルから構成されます。アクティブなトンネルには、BGP行の最後にネットマスクが表示されます。トンネルのステータスアイコンは制御目的のためにのみ表示されており、1つのトンネルを有効または無効にすることはできません。

すべてのAmazon VPCコネクションを無効にするには、一番上のトグルスイッチをクリックします。1つのコネクションを無効にするには、そのコネクションのトグルスイッチをクリックします。

接続を閉じてリストから削除するには、その接続の赤い削除アイコンをクリックします。

注 – コネクションはAmazon VPC側で設定されているため、以前と同じデータを使用することで削除したコネクションをSophos UTMに再度インポートできます。

Amazon VPCについての詳細は、Amazonユーザガイドをご確認ください。

15.1.2 セットアップ

*サイト間VPN > Amazon VPC > セットアップ*ページでは、Amazon VPC(バーチャルプライベートクラウド)に対するコネクションを追加できます。1つのAmazon Web Service(AWS)アカウントと、Sophos UTMのIPアドレスを*カスタマゲートウェイ*(VPC VPN接続のエンドポイントを指すAmazonの用語)として使用して設定されているすべてのコネクションをインポートするか、Amazonからダウンロードできる設定ファイルを使用して1つずつ接続を追加できます。

Amazon資格情報によるインポート

1つのAWSアカウントで設定したコネクションと、Sophos UTMのIPアドレスをカスタマゲートウェイとして使用して設定したコネクションをすべて一度にインポートすることができます。これには、単にAmazon Web Serviceアカウントの作成時に提供されたAWSのクレデンシャルを入力するだけです。

注 – *ステータス*タブにリストされた既存の全コネクションは、インポート中に削除されます。

接続をインポートするには、以下の手順に従います。

1. **次の設定を行います。**
   アクセスキー: AmazonアクセスキーIDを入力します。これは20文字の英数字シーケンスです。

   シークレットキー: シークレットアクセスキーを入力します。これは40文字のシーケンスです。

2. ***適用*をクリックします。**
   接続がインポートされ、*ステータス*ページに表示されます。

Amazon VPC設定によるインポート

既存の接続リストに1つの接続を追加するには、その接続の設定ファイルをアップロードする必要があります。

1つの接続をインポートするには、以下の手順に従います。

1. **Amazon VPC接続の設定ファイルをダウンロードします。**
   Amazonのダウンロードダイアログで、*ベンダー*ドロップダウンリストから*Sophos*を選択します。

2. *ファイルのアップロード***ダイアログボックスを開きます。**
   *VPC設定ファイル*ボックスの横にあるフォルダアイコンをクリックします。

3. **設定ファイルを選択してアップロードします。**
   選択したファイルをアップロードするには、*アップロード開始*ボタンをクリックします。

   ファイル名が*VPC設定ファイル*ボックスに表示されます。

4. **スタティックルートを使用している場合は、リモートネットワークを入力します。**
   リモートネットワークは、設定ファイルの一部ではありません。そのため、*リモートネットワーク*フィールドに、たとえば、10.0.0.0/8のように個別に入力する必要があります。このフィールドが重要であるのは、Amazon VPCで、ダイナミックルーティングの代わりにスタティックルートを使用するように設定した場合だけです。

5. *適用***をクリックします。**
   接続がインポートされ、*ステータス*ページに表示されます。

ルート伝播

Amazon VPC内で有効化されたルーティングテーブルをルート伝播でプッシュされるネットワークを設定できます。

ローカルネットワークを選択するには、次の手順に従います。

1. **ローカルネットワークを追加します。**
   ルート伝播でプッシュされるローカルネットワークを追加または選択します。*定義を追加する方法は、定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

2. *適用***をクリックします。**
   ルート伝播ネットワークが適用されます。

15.2 IPsec

*IPsec*とは、すべてのIPパケットを暗号化または認証すること(あるいはその両方)によってIP *インターネットプロトコル* 通信のセキュリティを維持するための標準です。

IPsec標準は、次の2つのサービスモードと2つのプロトコルを定義しています。

- トランスポートモード
- トンネルモード
- *AH 認証ヘッダ* 認証プロトコル
- *ESP カプセル化セキュリティペイロード* 暗号化(および認証)プロトコル

IPsecには、SA *セキュリティアソシエーション* と鍵配布を手動および自動で管理するための方法も用意されています。これらの特徴は、DOI *(解釈ドメイン)* で一元管理されています。

IPsecモード

IPsecは、トランスポートモードまたはトンネルモードで機能します。原則的に、ホスト間接続ではどちらのモードも使用できます。ただし、いずれかのエンドポイントがセキュリティゲートウェイである場合、トンネルモードを使用する必要があります。この UTM での IPsec VPN 接続では、常にトンネルモードが使用されます。

トランスポートモードでは、元のIPパケットは他のパケットにカプセル化されません。元のIPヘッダは維持され、パケットの残りの部分は平文のまま(AH)またはカプセル化されて(ESP)送信されます。パケット全体をAHで認証することも、ESPでペイロードをカプセル化して認証することもできます。いずれの場合も、元のヘッダは平文としてWAN経由で送信されます。

トンネルモードでは、パケットヘッダとペイロードの全体が新しいIPパケットにカプセル化されます。IPヘッダがIPパケットに追加され、宛先アドレスは受信側トンネルエンドポイントに設定されます。カプセル化パケットのIPアドレスは変更なしで維持されます。続いて、元のパケットがAHで認証されるか、ESPでカプセル化されて認証されます。

IPsecプロトコル

IPsecでは、IPレベルで安全に通信するために2つのプロトコルを使用します。

- **AH** 認証ヘッダ :パケット送信者を認証し、パケットデータの完全性を保証するためのプロトコル。
- **ESP** カプセル化セキュリティペイロード :パケット全体を暗号化し、そのコンテンツを認証するためのプロトコル。

AH 認証ヘッダ プロトコルは、パケットデータの信頼性と完全性をチェックします。さらに、送信者と受信者のIPアドレスが送信中に変更されていないことをチェックします。パケットは、*ハッシュベースのメッセージ認証コード*(HMAC)と鍵を使用して作成されたチェックサムを使用して認証されます。次のいずれかのハッシュアルゴリズムが使用されます。

- **MD5** メッセージダイジェスト、バージョン5 ：このアルゴリズムでは、任意のサイズのメッセージから128ビットのチェックサムが生成されます。このチェックサムはメッセージの指紋のようなもので、メッセージが変更されるとチェックサムも変わります。このハッシュ値は、デジタル署名またはメッセージダイジェストとも呼ばれます。
- **SHA-1** セキュアハッシュ ：このアルゴリズムではMD5と類似したハッシュが生成されますが、SHA-1ハッシュは長さが160ビットです。SHA-1は鍵がMD5より長いため、MD5より強力なセキュリティが実現します。

MD5と比較すると、SHA-1ハッシュは計算が難しく、生成に必要なCPU時間はより長くなります。もちろん、計算速度は、プロセッサの処理速度とSophos UTMで使用されるIPsec VPN 接続の数に依存します。

ESP *カプセル化 セキュリティペイロード* プロトコルには、暗号化以外に、送信者を認証し、パケットコンテンツを検証する機能もあります。トンネルモードで ESP を使用すると、IP パケット全体（ヘッダとペイロード）が暗号化されます。ここで、暗号化されていないIPヘッダとESPヘッダがカプセル化するパケットに追加されます。新しいIPヘッダには、受信側ゲートウェイと送信側ゲートウェイのアドレスが含まれています。これらのIPアドレスは、VPNトンネルのアドレスです。

暗号化付きのESPでは、通常次のアルゴリズムが使用されます。

- 3DES（トリプルデータ暗号化標準）
- AES（高度暗号化標準）

これらのうち、AESが最も安全です。AESで使用可能な鍵の有効長は128ビット、192ビット、256ビットです。Sophos UTMは、多数の暗号化アルゴリズムをサポートしています。認証にはMD5またはSHA-1アルゴリズムを使用できます。

NAT トラバーサル NAT-T

NATトラバーサルとは、NATデバイスを使用するTCP/IPネットワーク内のホスト間で接続を確立するための技術です。この接続は、ESPパケットのUDPカプセル化を使用して、NATデバイス経由でIPsecトンネルを確立することによって実現します。UDPカプセル化は、IPsecピア間でNATが検出された場合のみに使用されます。検出されなかった場合は、通常のESPパケットが使用されます。

NATトラバーサルにより、ゲートウェイまたはロードウォリアをNATルータの背後に配置しながら、IPsecトンネルを確立できるようになります。この機能を使用する場合、両方のIPsecピアでNATトラバーサルがサポートされている必要があります。ネゴシエーションは自動的に行われます。NATデバイスでIPseパススルーがオフになっていることを確認してください。オンになっていると、NATトラバーサルの使用に支障が出る可能性があります。

ロードウォリアでNATトラバーサルを使用したい場合、WebAdmin内の対応ユーザオブジェクトにスタティック(静的)なリモートアクセスIPアドレス(RASアドレス)が設定されている必要があります(WebAdminの*ユーザ*ページの*スタティックリモートアクセスIPを使用*も参照してください)。

データ未送信時に確立されたトンネルが期限切れになることを防ぐために、NATトラバーサルのkeep-alive信号がデフォルトで60秒間隔で送信されます。keep-aliveメッセージは、NATルータがセッションに関連するステート情報を維持しており、トンネルが開いたままであることを確認するために送信されます。

TOS

「サービスタイプ」ビット(TOSビット)は、IPヘッダにあるいくつかの4ビットフラグです。これらのビットは、どのタイプのサービス品質が必要であるかを転送アプリケーションがネットワークに伝えることを許可するため、*サービススタイプ*ビットと呼ばれています。

Sophos UTMへの IPsec 導入では、TOS の値は常にコピーされます。

15.2.1 コネクション

*サイト間VPN > IPsec > コネクション*タブでは、IPsecコネクションを作成および編集することができます。

IPsecコネクションを作成するには、次の手順に従います。

1. ***コネクション*タブで*新規IPsec コネクション*をクリックします。**
   *IPsec コネクションの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:このコネクションを説明する名前を入力してください。

   リモートゲートウェイ:リモートゲートウェイ定義を選択します。リモートゲートウェイは、*サイト間VPN > IPsec > リモートゲートウェイ*タブで設定します。

   ローカルインタフェース:IPsecトンネルのローカルエンドポイントとして使用されるインタフェースの名前を選択します。

   ポリシ:このIPsecコネクションのIPsecポリシを選択します。IPsecポリシは、*サイト間VPN > IPsec > ポリシ*タブで定義できます。

   ローカルネットワーク:VPNトンネル経由でアクセス可能にするローカルネットワークを選択または追加します。定義を追加する方法は、*定義とユーザ > ネットワーク定義 > ネットワーク定義*ページで説明しています。

自動ファイアウォールルール：このオプションを選択すると、この接続のトラフィックを許可するファイアウォールルールを自動的に追加することができます。ルールは、接続が有効になるとすぐに追加され、接続が切断されると削除されます。より厳格なIPsec接続を使用する場合は、*自動ファイアウォールルール*を使用しないで、代わりにファイアウォールルールセット内のIPsecオブジェクトを使用します。

厳密ルーティング：ストリクトルーティングを選択すると、VPNルーティングは(宛先IPアドレスのみではなく)送信元IPアドレスと宛先IPアドレスに従って実行されます。この場合、VPNトンネル定義と完全に一致するパケットのみがVPNトンネルにルーティングされます。この結果、SNATを使用して本来トンネル定義の一部ではないネットワークまたはホストをVPNトンネルに追加することはできません。一方、厳密ルーティングを使用しない場合、異なる送信元アドレスから同じネットワークに対して非暗号化/暗号化の混在するセットアップを行うことはできません。

ローカルインタフェースにバインド：デフォルトでは、このオプションの選択は解除されていて、選択したローカルネットワークから発生するすべてのトラフィックおよび定義されたリモートネットワークを宛先とするすべてのトラフィックは、必ずこのIPsecトンネルを経由して送信されます。セレクタが必ず同じになるので、異なるインタフェースで同一のトンネルを複数持つことはできません。ただし、有効にした場合には、定義されたIPsecセレクタは選択したローカルインタフェースに関連付けられます。したがって、スタティックルートでIPsecポリシをバイパスするか、異なるアップリンクで冗長IPsecトンネルを定義し、マルチパスルールを使用して、使用可能なインタフェースおよびそのIPsecトンネルでトラフィックのバランシングを行うことができます。この設定の使用例：

- スタティックルート経由でリモートネットワークに属しているローカルホストに対してIPsecポリシをバイパスする。
- 複数のIPsecトンネルまたは自動フェイルオーバーを備えているMPLSリンクに渡るマルチパスルールで、レイヤ3およびレイヤ4に基づくトラフィックのバランシングを行う。

注 – このオプションは、インタフェースグループと組み合わせて使用することはできません。

コメント(オプション)：説明などの情報を追加します。

3. ***保存*をクリックします。**
   新しい接続がIPsecの*コネクション*リストに表示されます。

接続を編集または削除するには、対応するボタンをクリックします。

ライブログを開く: IPsec VPNライブログには、確立されたIPsec接続に関するモニタリング情報が表示されます。ボタンをクリックして、新しいウィンドウでライブログを開きます。

15.2.2 リモートゲートウェイ

*サイト間VPN > IPsec > リモートゲートウェイ*タブでは、サイト間VPNトンネル用にリモートゲートウェイを定義できます。これらのリモートネットワーク定義は、*IPsec > コネクション*タブでIPsecコネクションを作成すると使用可能になります。

リモートゲートウェイを追加するには、次の手順に従ってください。

1. ***リモートゲートウェイ*タブで、*新規リモートゲートウェイ*をクリックします。**
   *リモートゲートウェイの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前: このリモートゲートウェイを説明する名前を入力してください。

   ゲートウェイタイプ: ゲートウェイのタイプを選択します。次のタイプを使用できます。

   - *イニシエートを行う*: リモートエンドポイントにスタティック(静的)IPアドレスがあり、リモートゲートウェイへの接続をゲートウェイによって開始できる場合に選択します。選択する場合、*ゲートウェイ*ボックスにリモートゲートウェイを指定します。このオプションは、リモートゲートウェイがDynDNSによって解決される場合にも選択できます。

   - *レスポンドのみ*: リモートエンドポイントのIPアドレスが不明であるか、DynDNSで解決できない場合に選択します。ゲートウェイはリモートゲートウェイへの接続を開始できず、応答のみを必要とする接続を受信するまで待機します。

   認証タイプ: このリモートゲートウェイ定義の認証タイプを選択します。次のタイプを使用できます。

   - **事前共有鍵**: *事前共有鍵*(PSK)による認証では、秘密のパスワードを鍵として使用します。これらのパスワードは、接続を確立する前にエンドポイントに配布する必要があります。新しいVPNトンネルが確立されると、両端で、相手側が秘密のパスワードを知っていることのチェックが行われます。PSKのセキュリティは、使用するパスワードの品質に依存します。一般的な言葉や成句では、辞書攻撃に対して脆弱です。常時の、または長期的なIPsecコネクションでは、パスワードの代わりに証明書を使用すべきです。

   - **RSA鍵**: RSA鍵を使用する認証は、より高度です。この方式では、公開鍵と秘密鍵から成る鍵ペアが接続の両端で生成されます。秘密鍵は、鍵交換時の暗号化と認証で必要です。この認証方式を使用するIPsecVPN接続の両エンドポイントは、独自の鍵ペアを必要とします。リモートユニットの公開RSA鍵(*サイト間VPN > IPsec >*

ローカルRSA鍵)をローカルユニットの*公開鍵*ボックスにコピーし、逆方向のコピーも行います。さらに、それぞれのRSA鍵に対応するVPN IDタイプとVPN識別子を入力します。

- *ローカル***X.509**証明書：同様に、X.509証明書による認証方式も公開鍵と秘密鍵を使用します。X.509証明書には、公開鍵と、鍵の所有者を特定する情報が含まれています。このような証明書は、信頼される*認証局*(CA)によって署名され、発行されたものです。鍵交換中に証明書が交換され、ローカル保存されたCA証明書を使用して認証されます。リモートゲートウェイのX.509証明書がユニットにローカル保存されている場合、この認証タイプを使用してください。

- *リモート***X.509**証明書：リモートゲートウェイのX.509証明書がユニットにローカル保存されていない場合、この認証タイプを使用してください。リモートユニットで使用されている証明書のVPN IDタイプとVPN識別子を選択する必要があります。この証明書は、*サイト間 VPN > IPsec > 詳細*タブの*ローカル X.509 証明書*エリアで選択されたものです。

VPN IDタイプ：認証タイプによっては、VPN IDタイプとVPN識別子を選択する必要があります。ここで入力するVPN識別子は、リモートサイトで設定した値と一致している必要があります。サイト間VPNトンネルの確立に2台のUTMアプライアンスを使用しているとします。ローカルユニットでの認証タイプとして*RSA 鍵*を選択する場合、VPN ID タイプと VPN 識別子がリモートユニットの*サイト間 VPN > IPsec > ローカル RSA 鍵*タブでの設定と一致している必要があります。次のVPN IDタイプを選択できます。

- **IP**アドレス
- ホスト名
- メールアドレス
- 識別子 **DN**：*リモートX.509証明書*認証のみで使用。
- すべて：*応答のみ*ゲートウェイタイプのデフォルト。

リモートネットワーク：リモートゲートウェイ経由でアクセス可能にするリモートネットワークを選択します。

コメント(オプション)：説明などの情報を追加します。

3. **必要に応じて、詳細設定を行います。**
以下の詳細設定は、影響を理解している場合にのみ行ってください。

パス**MTU**検出をサポート：PMTU(パス最大伝送単位)とは、送信されるデータパケットのサイズです。IPデータパケットは、送信元から宛先までのパスのどこでもフラグメンテーション

(断片化)を必要としない最大サイズにすることが望まれます。パス上の一部ルータにとって断片化しないで転送するには大き過ぎるデータパケットがある場合、そのルータはそれらを破棄して、*ICMP Destination Unreachable*メッセージを「fragmentation needed and DF set」を意味するコードとともに返します。送信元ホストは、そのようなメッセージを受信すると、そのパスに対して想定されるPMTUを減らします。
このオプションを有効にすると、サーバ側でPMTUが有効UTMになっている場合にがPMTUを有効化します。

輻輳シグナリングをサポート **ECN** :ECN(明示的な輻輳通知)とはインターネットプロトコルの拡張であり、ネットワーク輻輳のエンドツーエンドな通知をパケットのドロップなしで許可します。元のIPパケットのヘッダからIPsecパケットのヘッダにECN情報をコピーするには、このオプションを選択します。リモートエンドポイントおよび下位のネットワークと関与するルータがこれをサポートしている必要があります。

XAUTH クライアントモードの有効化:XAUTHとは、IPsec IKEの拡張であり、VPNゲートウェイでユーザ名とパスワードを使用してユーザを認証します。このリモートゲートウェイでの認証にXAUTHを使用するためには、このオプションを選択して、リモートゲートウェイの要求に従ってユーザ名とパスワード(2回)を入力します。

4. ***保存*をクリックします。**
   ゲートウェイ定義が *リモートゲートウェイ*リストに表示されます。

リモートゲートウェイ定義を編集または削除するには、対応するボタンをクリックします。

15.2.3 ポリシー

*IPsec > ポリシ*タブでは、IPsecコネクション用のパラメータをカスタマイズし、ポリシに統合することができます。IPsecポリシは、IPsec接続のIKE(インターネット鍵交換)とIPsecプロポーザルパラメータを定義します。それぞれのIPsec接続にはIPsecポリシが必要です。

注 – Sophos UTM は、IKE フェーズ 1 のメインモードのみをサポートしています。アグレッシブモードはサポートされていません。

IPsecポリシを作成するには、以下の手順に従います。

1. ***ポリシ*タブで、*新規IPsec ポリシ*をクリックします。**
   *IPsecポリシの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:このポリシを説明する名前を入力します。

IKE暗号化*アルゴリズム*:暗号化アルゴリズムでは、IKEメッセージの暗号化に使用するアルゴリズムを指定します。以下のアルゴリズムがサポートされています。

- *DES*(56ビット)
- *3DES*(168ビット)
- *AES 128*(128ビット)
- *AES 192*(192ビット)
- *AES 256*(256ビット)
- *Blowfish*(128ビット)
- *Twofish*(128ビット)
- *Serpent*(128ビット)

セキュリティに関する注記 – 弱いアルゴリズムであり、潜在的脆弱性を表しているため、DESを使うことを強く推奨します。

IKE認証*アルゴリズム* 認証アルゴリズムでは、IKEメッセージの完全性チェックに使用するアルゴリズムを指定します。以下のアルゴリズムがサポートされています。

- *MD5*(128ビット)
- *SHA1*(160ビット)
- *SHA2 256*(256ビット)
- *SHA2 384*(384ビット)
- *SHA2 512*(512ビット)

IKE SA *ライフタイム* この値には、IKE SA(セキュリティアソシエーション)が有効な期間(つまり次の鍵更新を行うタイミング)を秒単位で指定します。有効な値は60秒~28800秒(8時間)です。デフォルト値は7800秒です。

IKE DH*グループ* 接続をネゴシエートする際は、通信するパーティはデータの暗号化に使用する実際の鍵についても取り決めます。IKEはセッション鍵を生成するために、ランダムデータを利用する*Diffie-Hellman*(DH)アルゴリズムを使用します。ランダムデータの生成はプールビットに基づいて行われます。基本的にはIKEグループがプールビット数を知らせます。プールビット数が多いほど、ランダムな数字が大きくなります。数字が大きいほど、Diffie-Hellmanアルゴリズムの解読は難しくなります。結果として、プールビット数が多ければ安全

ですが、CPUリソースの消費量も増えます。現在は以下のDiffie-Hellmanグループがサポートされています。

- *グループ1 : MODP 768*
- *グループ2 : MODP 1024*
- *グループ5 : MODP 1536*
- *グループ14 : MODP 2048*
- *グループ15 : MODP 3072*
- *グループ16 : MODP 4096*

セキュリティに関する注記 **-** グループ1(MODP 768)は弱く、相互運用性の理由からのみサポートされています。潜在的脆弱性を表しているため、それを使うことを強く推奨します。

IPsec暗号化アルゴリズムIKEの場合と同じ暗号化アルゴリズム。さらに、以下のエントリもあります。

- *暗号化なし null*
- *AES 128 CTR*(128ビット)
- *AES 192 CTR*(192ビット)
- *AES 256 CTR*(256ビット)
- *AES 128 GCM 96ビット*
- *AES 192 GCM 96ビット*
- *AES 256 GCM 96ビット*
- *AES 128 GCM 128ビット*
- *AES 192 GCM 128ビット*
- *AES 256 GCM 128ビット*

セキュリティに関する注記 **–** これは潜在的脆弱性を表しているため、暗号化を使用しないか、DESを使用することを推奨いたします。

IPsec認証*アルゴリズム*：IKEの場合と同じ認証アルゴリズム。さらに、以下のアルゴリズムもあります。

- *SHA2 256*（96ビット）
- *SHA2 384*（96ビット）
- *SHA2 512*（96ビット）

これらは、RFC 4868に準拠しないトンネルエンドポイント、たとえばV8以前のUTM（例、ASGバージョンなど）への対応のために用意されています。そのため、96ビットより長い切り捨てられたチェックサムをサポートしません。

IPsec SA *ライフタイム*：この値には、IPsec SAが有効な期間（つまり次の鍵更新を行うタイミング）を秒単位で指定します。有効な値は60秒～86400秒（1日）です。デフォルト値は3600秒です。

IPsec PFS*グループ*：*Perfect Forward Secrecy*（PFS）という概念では、セッション鍵を使用できなくなった場合に、この特定セッションのデータにのみアクセスを許可します。PFSが存在するには、IPsec SAの保護に使用される鍵は、IKE SAの鍵を取得するために使用されるランダム鍵作成用のマテリアルから派生したものではないことが必要です。その場合、PFSは2回目のDiffie-Hellman鍵交換を開始し、IPsec接続に対して選択されたDHグループが新たにランダム生成された鍵を取得することを提案します。サポートされているDiffie-HellmanグループはIKEの場合と同じです。

PFSを有効にすると安全性が高まりますが、交換にさらに時間がかかるようになります。低速なハードウェアではPFSは使用しないことをお勧めします。

注 - PFSはすべてのベンダーとの完全な相互運用性はありません。ネゴシエーション時に問題が発生した場合は、PFSを無効にしてください。

厳密*ポリシー*：IPsecゲートウェイが暗号化アルゴリズムおよびその強度について提案を行うと、IPsecポリシがそれに対応していない場合でも、受信側ゲートウェイがこの提案を受け入れる場合があります。このオプションを選択すると、指定したパラメータを厳密にそのとおり使用することについてリモートエンドポイントが合意しないときは、IPsec接続は確立されません。UTMのIPsecポリシがAES-256暗号化を必要とする際に、SSH Sentinelを使用するロードウォリアがAES-128を使用して接続しようとすると、厳格なポリシオプションが有効である場合は、接続は拒否されます。

注 – 圧縮の設定は*厳格なポリシ*を介しては施行されません。

圧縮：このオプションでは、*IPペイロード圧縮プロトコル*（IPComp）によってIPパケットを暗号化の前に圧縮するかどうかを指定します。IPCompはIPパケットを圧縮してそのサイズを縮小し、通信ホストまたはゲートウェイのペア間の全体的な通信パフォーマンスを向上させます。デフォルトでは圧縮はオフになっています。

コメント（オプション）：説明などの情報を追加します。

3. *保存*をクリックします。
新しいポリシが*ポリシ*リストに表示されます。

ポリシーを編集または削除するには、対応するボタンをクリックします。

15.2.4 ローカルRSA鍵

RSA認証では、VPNエンドポイントの認証にRSA鍵が使用されます。エンドポイントの公開鍵は、接続が確立される前に手動で交換します。この認証タイプを使用する場合、VPN識別子を定義して、ローカルRSA鍵を作成する必要があります。ゲートウェイの公開RSA鍵を、Sophos UTMに対してIPsec RSA認証を使用するリモートIPsecデバイスで使用できるようにする必要があります。

現在のローカル公開RSA鍵

現在インストールされているローカルRSA鍵ペアの公開部分が表示されます。ボックスをクリックし、CTRL-AとCTRL-Cを押してクリップボードにコピーしてください。

ローカルRSA鍵VPNオプション

お客様のニーズに最適なVPN IDタイプを選択します。デフォルトでは、ゲートウェイのホスト名がVPN識別子として取得されます。スタティック（静的）IPアドレスをローカルVPNエンドポイントとする場合は、*IPアドレス*を選択します。あるいは、モバイル IPsec ロードウォリアの VPN ID としてメールアドレスを使用することもできます。

- ホスト名：デフォルト設定はゲートウェイのホスト名です。ただし、ここで他のホスト名を入力することもできます。
- メールアドレス：デフォルトでは、これはゲートウェイのadminアカウントのメールアドレスです。ただし、ここで他のメールアドレスを入力することもできます。
- IPアドレス：ゲートウェイの外部インタフェースのIPアドレス。

設定を保存するには*適用*をクリックします。設定を変更しても、RSA鍵に変化はありません。

ローカルRSA鍵の再生成

新しいRSA鍵を生成するには、希望する鍵サイズを選択し、*適用*をクリックします。これにより、鍵生成プロセスが開始します。選択した鍵の長さと使用しているハードウェアに応じて、処理には数分から最大2時間かかる場合があります。鍵サイズ(鍵の長さ)は、1つの暗号で使用可能な鍵の数の尺度です。長さは通常、ビットで指定します。次の鍵サイズがサポートされています。

- 1024 ビット
- 2048 ビット
- 4096 ビット

RSA鍵を生成すると、適切な公開鍵が*現在のローカル公開RSA鍵*ボックスに表示されます。新しいRSA鍵を生成すると、古い鍵が上書きされます。

15.2.5 詳細

*サイト間VPN > IPsec > 詳細*タブでは、IPsecVPNの詳細オプションを設定することができます。希望の認証タイプに応じて、ローカル証明書(X.509認証の場合)やローカルRSA鍵(RSA認証の場合)などを定義可能です。この設定は熟練ユーザのみが行ってください。

ローカルX.509証明書

X.509認証では、証明書を使用してVPNエンドポイントの公開鍵を検証します。この認証タイプを使用する場合は、*ローカルX.509証明書*エリアのドロップダウンリストからローカル証明書を選択する必要があります。選択した鍵/証明書は、X.509認証が選択された場合のリモートピアへのゲートウェイの認証に使用されます。

適切な秘密鍵がある証明書のみ選択できます。他の証明書はこのドロップダウンリストでは利用できません。

選択できる証明書がない場合、新しい証明書を作成するか、またはアップロード機能を使用してインポートして、*証明書管理*メニューで追加する必要があります。

証明書を選択したら、秘密鍵を保護するパスフレーズを入力します。パスフレーズは保存プロセスで確認され、パスフレーズが暗号化鍵と一致しない場合はエラーメッセージが表示されます。

アクティブな鍵/証明書を選択すると、それは*ローカルX.509証明書*エリアに表示されます。

デッドピア検出 DPD

デッドピア検出 **(DPD)** を使用:デッドピア検出オプションを使用して、リモートVPNゲートウェイあるいはクライアントに接続できない場合は接続を自動的に終了します。スタティックエンドポイントと

の接続では、トンネルは自動的に再ネゴシエートされます。ダイナミックエンドポイントとの接続では、リモート側でトンネルの再ネゴシエートを行うことが必要です。通常はこのオプションを常に有効にしておくほうが安全です。IPsecピアはリモート側がデッドピア検出をサポートするかどうかを自動的に判断し、必要に応じて通常モードにフォールバックします。

NATトラバーサル NAT-T

NATトラバーサルを使用:このオプションを選択すると、IPsecトラフィックは、*ネットワークアドレス変換*(NAT)を使用するアップストリームシステムを通過できるようになります。さらに、NATトラバーサルのキープアライブ間隔を定義できます。設定を保存するには*適用*をクリックします。

CRL処理

証明書のプロバイダが、まだ有効な証明書に与えられる承認を取り消す場合があるかもしれません。たとえば、証明書の受取人が不正なデータ(名前など)を使ってそれを不正に取得したことが判明した場合や、証明書に埋め込まれた公開鍵の一部である秘密鍵を攻撃者が入手した場合は、証明書が失効します。そのような場合に備えて、いわゆる*証明書失効リスト*(CRL)が使用されます。CRLには通常、依然として有効期間は残っているものの無効とされた証明書のシリアル番号が含まれています。

これらの有効期限が切れると、証明書は無効になり、ブロックリストから削除されます。

自動フェッチ:この機能は、HTTP、Anonymous(匿名)FTP、またはLDAPバージョン3を介しパートナー証明書で定義されたURLを通してCRLを要求します。有効期限が切れたら、要求によってCRLをダウンロードし、保存して更新できます。この機能を、ポート80または443を経由せずに使用する場合は、適切なファイアウォールルールを設定して、CRL配布サーバにアクセスできるようにしてください。

厳密ポリシー:このオプションを有効にすると、対応するCRLのないパートナー証明書は拒否されます。

PSKプローブ

応答のみモードを使用したIPsec接続では、それぞれのIPsec接続に対して別々の事前共有鍵(PSK)を使用することを選択できます。

PSKプローブの有効化:このチェックボックスにチェックを入れて、このオプションを有効にします。この設定は、L2TP-over-IPsec、リモートアクセスIPsec、VPN IPsecの各接続に影響を与えます。

15.2.6 デバッグ

IKEデバッグ

*IKEデバッグ*セクションでIKEデバッグオプションを設定できます。どのタイプのIKEメッセージまたは通信についてデバッグ出力を作成するかはチェックボックスで選択します。

注 – *IKEデバッグ*セクションは、*サイト間VPN IPsec*、*リモートアクセスIPsec*、*L2TP over IPsec*、および*Cisco VPN クライアント*メニューの *デバッグ*タブで同じものが使用されています。

以下のフラグをログできます。

- コントロールフロー: IKEステートのコントロールメッセージを表示します。
- 送信パケット: 送信IKEメッセージのコンテンツを表示します。
- 受信パケット: 受信IKEメッセージのコンテンツを表示します。
- カーネルメッセージ: カーネルとの通信メッセージを表示します。
- 冗長化: その他のHA ノードとの通信を表示します。

15.3 SSL

サイト間VPNトンネルはSSL接続を介して確立できます。SSL VPN接続には明確な役割があります。トンネルエンドポイントはクライアントまたはサーバとして機能します。常にクライアントが接続を開始し、サーバがクライアントの要求に応答します。これは、通常は両方のエンドポイントが接続を開始できるIPsecとは対照的です。

注 – 接続の確立に問題がある場合は、Webフィルタが透過モードで動作してSSLスキャンが有効になっているかどうかを確認してください。Webフィルタが透過モードで動作してSSLスキャンが有効になっている場合は、VPN接続のターゲットホストが*透過モードスキップリスト*(*Webプロテクション* > *フィルタオプション* > *その他*の下)に追加されていることを確認してください。

15.3.1 コネクション

SSLVPNサイト間トンネルを作成するには、最初にサーバ設定を作成することが必要です。クライアントの設定は、常に2番目のステップで行います。

サーバ設定を作成するには、以下の手順に従います。

1. ***コネクション*タブで、*新規SSLコネクション*をクリックします。**
   *SSLコネクションの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   コネクションタイプ: ドロップダウンリストから*サーバ*を選択します。

   コネクション名 : コネクションを説明する名前を入力します。

   スタティック仮想IPアドレスを使用（オプション）: このオプションは、IPアドレスプールがクライアントのネットワーク環境と互換でない場合のみ選択します。デフォルトでは、クライアントには*仮想IPプール*（*設定*タブで設定）からIPアドレスが割り当てられます。まれに、そのようなIPアドレスが、既にクライアントホストで使用されている場合があります。そのような場合は、*スタティックピアIP*フィールドに適切なIPアドレスを入力します。このIPアドレスは、トンネルセットアップ時にクライアントに割り当てられます。

   ローカルネットワーク: リモートからのアクセスを許可する1つ以上のローカルネットワークを選択または追加します。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

   リモートネットワーク: ローカルネットワークへの接続を許可する1つ以上のリモートネットワークを選択または追加します。

   > 注 – *ローカルネットワーク*と*リモートネットワーク*の設定は、後でクライアントの設定をやり直さずに変更できます。

   自動ファイアウォールルール（オプション）: 有効にすると、UTMは、アクセスするすべてのSSL VPNクライアントに対し、選択されたローカルネットワークへのアクセスを自動的に許可します。

   コメント（オプション）: 説明などの情報を追加します。

3. ***保存*をクリックします。**
   新しいSSLサーバコネクションが*コネクション*リストに表示されます。

4. **設定ファイルをダウンロードします。**
   新しく作成したSSLサーバコネクションの行にある*ダウンロード*ボタンを使用して、この接続のクライアント設定ファイルをダウンロードします。

   設定ファイルの暗号化（オプション）: セキュリティのために設定ファイルを暗号化することをお勧めします。パスワードを2回入力します。

   *ピア設定のダウンロード*をクリックしてファイルを保存します。

このファイルは、クライアント側の管理者がトンネルのクライアントエンドポイントをセットアップする際に必要になります。

次のステップはクライアントの設定で、これはサーバ側ではなくクライアント側で行います。ダウンロードしたクライアント設定ファイルが手元にあることを確認してください。

クライアント設定を作成するには、以下の手順に従います。

1. ***コネクション*タブで、*新規SSLコネクション*をクリックします。**
   *SSLコネクションの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   コネクションタイプ:ドロップダウンリストから*クライアント*を選択します。

   コネクション名:コネクションを説明する名前を入力します。

   設定ファイル:フォルダアイコンをクリックし、クライアント設定ファイルを探して*アップロード開始*をクリックします。

   パスワード(オプション):ファイルが暗号化されている場合は、パスワードを入力します。

   HTTPプロキシサーバを使用(オプション):クライアントがプロキシの背後にある場合は、このチェックボックスにチェックを入れ、プロキシの設定を入力します。

   プロキシは認証が必要(オプション):プロキシに対するクライアントの認証が必要な場合は、このチェックボックスにチェックを入れ、ユーザ名とパスワードを入力します。

   ピアホスト名を上書き(オプション):サーバシステムの通常のホスト名(またはDynDNSホスト名)をクライアントホストで解決できない場合は、このチェックボックスにチェックを入れ、ホスト名をここに入力します。

   自動ファイアウォールルール(オプション):有効にすると、UTMは、トンネル化ローカルネットワークとトンネル化リモートネットワーク上のホスト間のトラフィックを自動的に許可します。

   コメント(オプション):説明などの情報を追加します。

3. ***保存*をクリックします。**
   新しいSSL VPNクライアントコネクションが*コネクション*リストに表示されます。

クライアントコネクションを編集または削除するには、対応するボタンをクリックします。

*サイト間VPN*メニューをクリックすると、概要ページにSSL VPNコネクションのステータスが表示されます。コネクションが確立すると、ステータスアイコンが緑色に変わります。その後、トンネル両側の相互接続されたサブネットに関する情報も参照可能になります。

15.3.2 設定

*SSL > 設定*タブで、SSL VPN サーバー接続の基本設定を設定できます。

注 – このタブは*サイト間 VPN > SSL*および*リモートアクセス > SSL*で同じです。ここで加えた変更は、常に両方のSSL設定に影響を与えます。

サーバ設定

SSLVPN 接続について以下の設定を行うことができます。

- インタフェースアドレス: デフォルトは*すべて*です。Webアプリケーションファイアウォールを使用する場合、サービスがSSL接続をリスンするためのインタフェースアドレスを指定する必要があります。サイト間/リモートアクセスSSL接続ハンドラとWebアプリケーションファイアウォールが受信SSL接続を識別できるようにするために、この設定が必要です。
- プロトコル: 使用するプロトコルを選択します。*TCP*または*UDP*を選択できます。
- ポート: ポートを変更できます。デフォルトは`443`です。ポート`10443`、SUM ゲートウェイマネージャポート`4422`、または WebAdmin インタフェースが使用しているポートは使用できません。
- ホスト名を上書き: *ホスト名を上書き*ボックスの値は、クライアントVPN接続のターゲットホスト名として使用され、デフォルトではゲートウェイのホスト名になります。システムの通常のホスト名(またはDynDNSホスト名)にこの名前でインターネットから到達できない場合のみ、デフォルトを変更します。

仮想IPプール

プールネットワーク: これは、特定のIP範囲からSSLクライアントにIPアドレスを配布するために使用される仮想IPアドレスプールです。デフォルトでは、*VPNプール SSL* が選択されています。別のアドレスプールを選択する場合は、ネットマスクを29ビット以下にする必要があります。この理由は、OpenVPN はネットマスクが`/30`、`/31`、または`/32`のアドレスプールを扱えないからです。ネットマスクは最低16に制限されていることに注意してください。

Duplicate 重複 CN

ユーザが異なるIPアドレスから同時に接続できるようにする場合は、*1ユーザ当たりの複数同時接続を許可*を選択します。無効にすると、ユーザあたり1つの同時SSL VPN接続のみが可能になります。

15.3.3 詳細

*SSL > 詳細*タブで、暗号化設定、圧縮設定、デバッグ設定など、各種の高度なサーバーオプションを設定できます。

注 – このタブは*サイト間 VPN > SSL*および*リモートアクセス > SSL*で同じです。ここで加えた変更は、常に両方のSSL設定に影響を与えます。

暗号化設定

これらの設定で、すべてのSSL VPNリモートアクセスクライアントの暗号化パラメータを制御します。

- *暗号化アルゴリズム:* 暗号化アルゴリズムは、VPNトンネルを通して送信されるデータの暗号化に使用するアルゴリズムを指定します。以下のアルゴリズムがサポートされています。これらはすべて*暗号ブロック連鎖*(CBC)モードで動作します。
  - *DES-EDE3-CBC*
  - *AES-128-CBC*(128 ビット)
  - *AES-192-CBC*(192 ビット)
  - *AES-256-CBC*(256 ビット)
  - *BF-CBC*(Blowfish(128 ビット))
- *認証アルゴリズム:* 認証アルゴリズムは、VPNトンネルを通して送信されるデータの完全性チェックに使用するアルゴリズムを指定します。以下のアルゴリズムがサポートされています。
  - *MD5*(128ビット)
  - *SHA1*(160ビット)
  - *SHA2 256*(256ビット)
  - *SHA2 384*(384ビット)
  - *SHA2 512*(512ビット)
- *鍵サイズ:* 鍵サイズ(鍵の長さ)とは、Diffie-Hellman鍵交換の長さです。鍵が長ければ長いほど、対称鍵はセキュアになります。長さはビット単位で指定します。1024ビットまたは2048ビットの鍵サイズを選択できます。

- サーバ証明書：SSL VPNサーバがクライアントに対して自らの身元を証明するために使用するローカルSSL証明書を選択します。
- 鍵の有効期限：鍵の有効期限を入力します。デフォルトは28,800秒です。

圧縮設定

SSL VPN トラフィックの圧縮：有効にすると、SSL VPNトンネルを通して送信されるすべてのデータは、暗号化の前に圧縮されます。

デバッグ設定

デバッグモードの有効化：デバッグモードを有効にすると、デバッグに役立つ多くの情報がSSL VPNログファイルに含まれます。

15.4 証明書管理

*サイト間VPN > 証明書管理*メニューは、Sophos UTMの証明書関連のあらゆる操作を一元管理する場所です。中でも、X.509証明書の作成またはインポートや、*証明書失効リスト*(CRL)のアップロードなどを行うことができます。

15.4.1 証明書

*サイト間VPN > 証明書管理 > 証明書*タブで、X.509標準形式で公開鍵証明書を作成またはインポートできます。こうした証明書はデジタル署名された説明書で、通常は*認証局*(CA)が公開鍵および X.500 表記法による特定の*識別名*(DN)とともに発行します。

このタブで作成するすべての証明書には、RSA鍵が含まれています。これは、WebAdminインタフェースへの初回ログイン時に提供した情報を使用して、自動的に作成された自己署名認証局*VPNに署名するCA*によって自己署名されます。

証明書を生成するには、以下の手順に従います。

1. ***証明書*タブで、*新規証明書*をクリックします。**
   *証明書の追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前：この証明書を説明する名前を入力します。

   方式：証明書を作成するには、*生成*を選択します(証明書のアップロードに関する詳細は、以下を参照してください)。

鍵サイズ:RSA鍵の長さです。鍵が長いほど、より安全になります。1024ビット、2048ビット、4096ビットの鍵サイズを選択できます。使用する予定のアプリケーションプログラムやハードウェアデバイスと互換性がある鍵の最大サイズを選択します。より長いキーが特定の目的で重大なパフォーマンスの問題を引き起こさない限り、パフォーマンスを最適化するために鍵のサイズを減らさないでください。

VPN IDタイプ: 証明書には一意の識別子を定義する必要があります。以下のタイプの識別子を使用できます。

- メールアドレス
- ホスト名
- IPアドレス
- 識別名(DN):

VPN ID:選択したVPNIDタイプに応じて、このテキストボックスに適切な値を入力します。たとえば、*VPN IDタイプ*リストから*IPアドレス*を選択した場合、このテキストボックスにIPアドレスを入力します。*VPN IDタイプ*リストから*識別名*を選択した場合は、このテキストボックスは非表示になります。

ドロップダウンリストおよび*国*から*メール*までのテキストボックスを使用して、証明書の所持者を特定する情報を入力します。この情報は*識別名*を作成するために使用されます。つまり、その公開鍵を証明書が識別する団体の名前になります。この名前はX.500標準の多数の個人情報を含み、インターネット上で一意であると想定されます。証明書がロードウォリア接続用である場合は、*一般名*ボックスにユーザ名を入力します。証明書がホスト用である場合は、ホスト名を入力します。

コメント(オプション):説明などの情報を追加します。

3. ***保存*をクリックします。**
   証明書が*証明書*リストに表示されます。

証明書を削除するには、それぞれの証明書の*削除*ボタンをクリックします。

または、証明書をアップロードするには、以下の手順に従います。

1. ***証明書*タブで、*新規証明書*をクリックします。**
   *証明書の追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:この証明書を説明する名前を入力します。

   方式:*アップロード*を選択します。

ファイルタイプ: 証明書のファイルタイプを選択します。以下のいずれかのタイプの証明書をアップロードできます。

- **PKCS#12 (Cert+CA):**PKCSは、RSAラボラトリにより考案され*公開された公開鍵暗号標準*(PKCS)のグループです。PKCS#12ファイル形式は一般的に、秘密鍵を公開鍵証明書とともにコンテナのパスフレーズで保護して保存するために使用されます。この形式のファイルをアップロードするには、このコンテナパスフレーズを知っていることが必要です。
- **PEM Cert***のみ* :パスワード不要のBase64エンコードの*プライバシ強化メール*(PEM)ファイル形式。

ファイル: *ファイル*ボックスの隣りのフォルダアイコンをクリックし、アップロードする証明書を選択します。

コメント(オプション):説明などの情報を追加します。

3. ***保存*をクリックします。**
証明書が*証明書*リストに表示されます。

証明書を削除するには、それぞれの証明書の*削除*ボタンをクリックします。

証明書はPKCS#12またはPEM形式でダウンロードできます。PEMファイルは証明書だけを含みます。一方PKCS#12ファイルは、秘密鍵と署名に使用されたCA証明書を含んでいます。

15.4.2 認証局

*サイト間VPN > 証明書管理 > 認証局*タブで、ユニットに新しい*認証局*を追加できます。一般的に、*認証局*(CA)は、他のパーティが使用するデジタル証明書を発行する機関です。CAは、証明書に含まれる公開鍵が、その証明書に記載された人、組織、ホスト、あるいは他のエンティティに属することを、CA自身の証明書の秘密鍵を使って証明書の署名要求に署名することで証明します。このため、そのようなCAは署名CAと呼ばれます。

UTMでは、署名CAは、UTMへの最初のログイン時に提供した情報を使って自動的に作成されます。このように、*証明書*タブで作成するすべての証明書は、自己署名の証明書です。つまり、発行者と対象は同じになります。代わりに、サードパーティベンダの署名CAをインポートすることもできます。さらに、IPsec接続を要求するホストやユーザの真正性を確認する際に、秘密鍵が不明な別のCA証明書を使用することもできます。これらのCA証明書は確認CAと呼ばれ、このタブで追加できます。

重要 – 使用しているシステムで複数の検証CAを持つことはできますが、署名CAは1つだけしか持つことができません。新しい署名CAをアップロードすると、以前インストールされた署名CAは自動的に検証CAになります。

CAを追加するには、以下の手順に従います。

1. ***認証局*タブで、*新規CA*をクリックします。**
   *CAを追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前: このCAを説明する名前を入力します。

   タイプ: インポートするCAのタイプを選択します。検証CAと署名CAのいずれかを選択できます。確認 CA は PEM 形式で、署名 CA は PKCS#12 形式で利用できます。

   CA証明書: *CA証明書*ボックスの隣りのフォルダアイコンをクリックし、アップロードする証明書を選択します。新しい署名CAをアップロードする場合は、PKCS#12コンテナに使用されていたパスワードを入力する必要があります。

   コメント(オプション): 説明などの情報を追加します。

3. ***保存*をクリックします。**
   新しいCA証明書が*認証局*リストに表示されます。

CAを削除するには、それぞれのCAの*削除*ボタンをクリックします。

署名CAはPKCS#12形式でダウンロードできます。次にパスワードの入力を促すプロンプトが表示されます。このパスワードを使用してPKCS#12コンテナのセキュリティが保護されます。また、検証CAはPEM形式でダウンロードできます。

15.4.3 証明書失効リスト(CRL)

CRLは、失効したために使用できない証明書(正確にはシリアル番号)のリストです。*サイト間VPN > 証明書管理 > 証明書失効リスト(CRL)*タブで、PKIで使用しているCRLをアップロードできます。

CRLを追加するには、以下の手順に従います。

1. ***失効リスト(CRL)*タブで、*新規CRL*をクリックします。**
   *CRLの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**

名前：このCRLを説明する名前を入力します。

CRL *ファイル*：*CRLファイル*ボックスの隣りのフォルダアイコンをクリックし、アップロードするCRLを選択します。

コメント（オプション）：説明などの情報を追加します。

3. *保存*をクリックします。
新しいCRLが失効リストの一覧に表示されます。

CRLを削除するには、それぞれのCRLの*削除*ボタンをクリックします。

15.4.4 詳細

サイト間VPN > *証明書管理* > *詳細*タブでは、ユニットの初期セットアップ時に作成されたVPN署名CAを再生成できます。VPN署名CAは、リモートアクセスやサイト間VPN接続に使用されるデジタル証明書に署名する認証局です。古いVPN署名CA は、検証CAとして保持されます。

署名CAの再生成

現在の署名CAを使用してすべてのユーザ証明書を更新できます。この機能は*認証局*タブで別のVPN署名CAをインストールしたときに使用します。

> **警告** –UTMおよびすべてのユーザ証明書は、新しい署名CAを使用して、再作成することができます。これは、証明書ベースのサイト間およびリモートアクセスVPN接続を破壊します。

16 リモートアクセス

この章では、Sophos UTMのリモートアクセス設定の構成方法について説明します。Sophos UTMこの章では、のリモートアクセス設定の構成方法について説明します。*を使用したリモートアクセスは*、*Virtual Private Network VPN* によって実現します。VPNは、テレコミューティング従業員などのリモートユーザに企業ネットワークへのアクセスを提供するためのセキュアでコスト効果の高い方法です。VPN は IPsec や PPTP などの暗号化トンネリングプロトコルを使用して、VPN で伝送されるデータの機密性とプライバシーを保護します。

クロスリファレンス – リモートアクセスVPN接続の設定方法の詳細は、Sophos Knowledgebaseを参照してください。

UTMは、それぞれのリモートアクセス接続タイプに必要なインストールおよび設定ファイルを自動的に生成します。これらのファイルはユーザーポータルから直接ダウンロードできます。ただし、ユーザーには、使用可能な接続タイプに対応するファイルのみが提供されます。たとえば、SSL リモートアクセスを使用できるユーザーには、SSL インストールファイルのみが提供されます。

注 – すべてのユーザまたは選択したユーザのリモートアクセス設定ファイルは、*定義とユーザ* > *ユーザとグループ* > *ユーザ*タブでダウンロードできます。

*リモートアクセスステータス*ページには、全オンラインユーザの概要が含まれます。

この章には次のトピックが含まれます。

- SSL
- PPTP
- L2TP over IPsec
- IPsec
- HTML5 VPNポータル
- Cisco VPNクライアント
- 詳細
- 証明書管理

16.1 SSL

Sophos UTMのリモートアクセスSSL機能は、フル機能のSSLVPNソリューションであるOpenVPNによって実現します。これにより、お客様の会社とリモート従業員の間でポイントツーポイントの暗号化トンネルを作成することが可能になります。この機能では、インターネットリソースへのアクセスを許可するために、SSL証明書およびユーザ名/パスワードの組み合わせを必要とします。さらに、許可された各ユーザは、セキュアなユーザポータルから、カスタマイズされたSSL VPNクライアントソフトウェアバンドルをダウンロードできます。このバンドルには、無料のSSL VPNクライアント、SSL証明書、および簡単なワンクリックでインストールできる設定が含まれています。このSSL VPNクライアントは、ネイティブOutlook、ネイティブWindowsファイル共有などのほとんどのビジネスアプリケーションをサポートしています。

クロスリファレンス –SSL VPNクライアントの使用方法に関する詳細は、Sophos Knowledgebaseを参照してください。

16.1.1 プロファイル

リモートアクセス > *SSL* > *プロファイル*タブでは、リモートアクセスユーザの別のプロファイルを作成して、SSL VPNアクセスの基本設定を定義することができます。

SSL VPNプロファイルを設定するには、以下の手順に従います。

1. ***プロファイル*タブで、*新規 リモートアクセスプロファイル*をクリックします。**
   *リモートアクセスプロファイルの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   プロファイル名：このプロファイルを説明する名前を入力します。

   ユーザとグループ：このプロファイルでSSL VPNリモートアクセスを使用できるようにするユーザとユーザグループを選択するか、新しいユーザを追加します。ユーザを追加する方法は、*定義とユーザ* > *ユーザとグループ* > *ユーザ*ページで説明しています。

   ローカルネットワーク：VPN SSLトンネル経由で、選択したSSLクライアントに到達可能にするローカルネットワークを選択します。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

> 注 – デフォルトで、Sophos UTMのSSLVPNソリューションは、いわゆるスプリットトンネリングを採用しています。これは、リモートVPNユーザにVPN上のリソースへのアクセスを許可すると同時に、インターネットなどのパブリックネットワークへのアクセスを許可するプロセスです。ただし、以下の *ローカルネットワーク* フィールドで *すべて* を選択すると、スプリットトンネリングをバイパスできます。その結果、すべてのトラフィックがVPN SSLトンネル経由でルーティングされます。この場合、ユーザにパブリックネットワークへのアクセスを許可するかどうかは、ファイアウォールの設定によって決まります。

自動 *ファイアウォールルール*：このオプションを選択すると、この接続のプロファイルのトラフィックを許可するファイアウォールルールを自動的に追加できます。ルールは、プロファイルが有効になるとすぐに追加され、プロファイルが無効になると削除されます。このオプションを選択しない場合は、適切なファイアウォールルールを手動で指定する必要があります。

コメント（オプション）：説明などの情報を追加します。

3. ***保存*をクリックします。**
新しいプロファイルが *プロファイル* リストに表示されます。

プロファイルを編集または削除するには、対応するボタンをクリックします。

> 注 – ユーザポータルの *リモートアクセス* メニューが使用できるのは、*ユーザとグループ* ボックスで選択され、UTMにユーザ定義が存在するユーザの場合だけです（*定義とユーザ* > *ユーザとグループ* > *ユーザを参照*）。ユーザポータルへのログインに成功した認証されたユーザには、SSL VPNクライアントソフトウェアバンドルに加えてインストール手順（Sophos Knowledgebaseで提供）へのリンクが提供されます。CA証明書がインストールされていない場合、ホスト名がポータル証明書の一般名と一致しない場合、Androidの一部のブラウザでダウンロードが失敗することがあります。この場合、CA 証明書をインストールするか、他のブラウザを試します。

ライブログを開く

VPN ライブログを開く は、リモートアクセスアクティビティをログします。ボタンをクリックして、新しいウィンドウでライブログを開きます。

16.1.2 設定

SSL > *設定* タブで、SSL VPN サーバー接続の基本設定を設定できます。

注 – このタブは*サイト間 VPN* > *SSL*および*リモートアクセス* > *SSL*で同じです。ここで加えた変更は、常に両方のSSL設定に影響を与えます。

サーバ設定

SSLVPN 接続について以下の設定を行うことができます。

- インタフェースアドレス: デフォルトは*すべて*です。Webアプリケーションファイアウォールを使用する場合、サービスがSSL接続をリスンするためのインタフェースアドレスを指定する必要があります。サイト間/リモートアクセスSSL接続ハンドラとWebアプリケーションファイアウォールが受信SSL接続を識別できるようにするために、この設定が必要です。
- プロトコル: 使用するプロトコルを選択します。*TCP*または*UDP*を選択できます。
- ポート: ポートを変更できます。デフォルトは`443`です。ポート`10443`、SUM ゲートウェイマネージャポート`4422`、または WebAdmin インタフェースが使用しているポートは使用できません。
- ホスト名を上書き: *ホスト名を上書き*ボックスの値は、クライアントVPN接続のターゲットホスト名として使用され、デフォルトではゲートウェイのホスト名になります。システムの通常のホスト名(またはDynDNSホスト名)にこの名前でインターネットから到達できない場合のみ、デフォルトを変更します。

仮想IPプール

プールネットワーク: これは、特定のIP範囲からSSLクライアントにIPアドレスを配布するために使用される仮想IPアドレスプールです。デフォルトでは、*VPNプール (SSL)* が選択されています。別のアドレスプールを選択する場合は、ネットマスクを29ビット以下にする必要があります。この理由は、OpenVPN はネットマスクが`/30`、`/31`、または`/32`のアドレスプールを扱えないからです。ネットマスクは最低16に制限されていることに注意してください。

Duplicate 重複 CN

ユーザが異なるIPアドレスから同時に接続できるようにする場合は、*1ユーザ当たりの複数同時接続を許可*を選択します。無効にすると、ユーザあたり1つの同時SSL VPN接続のみが可能になります。

16.1.3 詳細

SSL > *詳細*タブで、暗号化設定、圧縮設定、デバッグ設定など、各種の高度なサーバーオプションを設定できます。

注 – このタブは*サイト間 VPN > SSL*および*リモートアクセス > SSL*で同じです。ここで加えた変更は、常に両方のSSL設定に影響を与えます。

暗号化設定

これらの設定で、すべてのSSL VPNリモートアクセスクライアントの暗号化パラメータを制御します。

- 暗号化アルゴリズム: 暗号化アルゴリズムは、VPNトンネルを通して送信されるデータの暗号化に使用するアルゴリズムを指定します。以下のアルゴリズムがサポートされています。これらはすべて*暗号ブロック連鎖*(CBC)モードで動作します。
    - *DES-EDE3-CBC*
    - *AES-128-CBC*(128ビット)
    - *AES-192-CBC*(192ビット)
    - *AES-256-CBC*(256ビット)
    - *BF-CBC*(Blowfish(128ビット))
- 認証アルゴリズム: 認証アルゴリズムは、VPNトンネルを通して送信されるデータの完全性チェックに使用するアルゴリズムを指定します。以下のアルゴリズムがサポートされています。
    - *MD5*(128ビット)
    - *SHA1*(160ビット)
    - *SHA2 256*(256ビット)
    - *SHA2 384*(384ビット)
    - *SHA2 512*(512ビット)
- 鍵サイズ: 鍵サイズ(鍵の長さ)とは、Diffie-Hellman鍵交換の長さです。鍵が長ければ長いほど、対称鍵はセキュアになります。長さはビット単位で指定します。1024ビットまたは2048ビットの鍵サイズを選択できます。
- サーバ証明書: SSL VPNサーバがクライアントに対して自らの身元を証明するために使用するローカルSSL証明書を選択します。
- 鍵の有効期限: 鍵の有効期限を入力します。デフォルトは28,800秒です。

圧縮設定

SSL VPN トラフィックの圧縮：有効にすると、SSL VPNトンネルを通して送信されるすべてのデータは、暗号化の前に圧縮されます。

デバッグ設定

デバッグモードの有効化：デバッグモードを有効にすると、デバッグに役立つ多くの情報がSSL VPNログファイルに含まれます。

16.2 PPTP

PPTP（*Point-to-Point Tunneling Protocol*）により、単一のインターネットベースのホストは、暗号化トンネルを通して内部ネットワークサービスにアクセスすることが可能になります。PPTPの設定は容易で、Microsoft Windowsシステムでは特別なクライアントソフトウェアは必要ありません。

PPTPはWindows 95 以降のMicrosoft Windowsバージョンに含まれています。PPTP をSophos UTMで使用するには、クライアントコンピュータがMSCHAPv2 認証プロトコルをサポートすることが必要です。Windows 95および98のユーザがこのプロトコルをサポートするには、システムに更新パッケージを適用する必要があります。

16.2.1 グローバル

グローバルPPTPオプションを設定するには、以下の手順に従います。

1. ***グローバル*タブで、PPTPリモートアクセスを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、*メイン設定*エリアが編集可能になります。

2. **次の設定を行います。**
   認証要求先：認証メカニズムを選択します。PPTPリモートアクセスは、ローカル認証とRADIUS認証のみをサポートします。

   - ローカル：*ローカル*を選択した場合は、PPTPリモートアクセスを使用できるユーザやユーザグループを指定します。バックエンドのユーザグループをフィールドにドラッグすることはできません。ユーザアカウントを指定するまでは、PPTPリモートアクセスはアクティブにできません。

注 – 選択したユーザのユーザ名およびパスワードには、ASCII印字可能文字[1]だけが含まれています。

注 – SSL VPN同様、ユーザポータルの *リモートアクセス* メニューにアクセスできるのは、*ユーザとグループ* ボックスで選択されたユーザと、ユーザ定義がUTMに定義されているユーザのみです。許可されたユーザがユーザポータルにログインすると、SophosKnowledgebaseにあるインストール手順へのリンクがあります。

- **RADIUS**: *RADIUS* は、RADIUSサーバを事前に設定している場合にのみ選択できます。この認証方法では、ユーザは外部RADIUSサーバに対して認証されます。このサーバは *定義とユーザ* > *認証サービス* > *サーバ* タブで設定できます。*ユーザとグループ* ダイアログボックスがグレーアウト表示されます。この設定はまだ変更できますが、影響はありません。RADIUSサーバはMSCHAPv2チャレンジ/応答認証をサポートする必要があります。サーバはクライアントのIPアドレスやDNS/WINSサーバアドレスなどのパラメータを戻すことができます。モジュールは、NAS-IDとして、次の文字列をRADIUSサーバに送信します。`pptp`。RADIUS認証を選択した場合は、ローカルユーザはPPTPでは認証できなくなることに注意してください。さらに、クライアントはMSCHAPv2認証もサポートする必要があることにも注意してください。

IP アドレスの割り当て: IPアドレスは、事前に定義したIPアドレスプールから割り当てることも、DHCPサーバを使用して自動的に配布することもできます。

- **IP アドレスプール**: PPTPによってリモートアクセスするクライアントに特定のIP範囲からIPアドレスを割り当てる場合は、このオプションを選択します。デフォルトでは、プライベートIPスペース`10.242.1.0/24`のアドレスが割り当てられます。このネットワーク定義は *VPNプール (PPTP)* と呼ばれ、すべてのネットワーク固有の設定オプションで使用できます。異なるネットワークを使用する場合は、*VPNプール (PPTP)* の定義を *定義とユーザ* > *ネットワーク定義* ページで変更します。または、*プールネットワーク* テキストボックスの隣りの「＋」アイコンをクリックして、別のIPアドレスプールを作成することもできます。ネットマスクは最低16までに制限されていることに注意してください。

- **DHCP サーバ**: *DHCP サーバ* を選択する場合、DHCPサーバが接続に使用するネットワークインタフェースも指定する必要があります。DHCPサーバーはインタフェースに直接接続する必要はありません。ルータを介してもアクセスできます。ローカル

[1] http://en.wikipedia.org/wiki/ASCII#ASCII_printable_characters

DHCP サーバーはサポートされません。ここで選択したDHCP サーバーは、物理的に異なるシステム上で稼働している必要があります。

3. ***適用*をクリックします。**
   設定が保存されます。

   トグルスイッチが緑色に変わります。

ライブログ

*PPTPデーモンライブログ*は、すべてのPPTPリモートアクセスアクティビティをログします。ボタンをクリックして、新しいウィンドウでライブログを開きます。

16.2.2 iOSデバイス

ユーザポータルでiOSデバイスユーザに対しPPTPの自動設定を提供することができます。

ただし、*グルーバル*タブの*ユーザーとグループ*ボックスに追加されたユーザーのみに対して、ユーザーポータルサイトに設定ファイルが表示されます。iOS デバイスのステータスはデフォルトで有効になっています。

コネクション名：PPTPコネクションを説明する名前を入力し、iOSデバイスのユーザがどのコネクションを確立しようとしているのか識別できるようにします。デフォルトの名前は、お客様の会社名の後にPPTP プロトコルが続いたものになります。

注 – *コネクション名*はすべての iOS デバイス設定（PPTP、L2TP over IPsec、Cisco VPN Client）で一意である必要があります。

ホスト名を上書き：システムのホスト名をクライアントがパブリックに解決できない場合は、ここにサーバのホスト名を入力して、これによって*システムのDNSホスト名*の前の*DynDNSホスト名*の内部プリファレンスを上書きします。

iOS デバイスの自動設定を無効にするには、トグルスイッチをクリックします。

トグルスイッチはグレーになります。

16.2.3 詳細

*リモートアクセス > PPTP > 詳細*タブで、暗号化の強度とPPTPリモートアクセスに関するデバッグ出力量を設定できます。PPTPの詳細オプションは、PPTPリモートアクセスのステータスが*グローバル*タブで有効になっていないと設定できません。

暗号強度

強い（128ビット）または弱い（40ビット）トンネル暗号化を選択できます（MPPE）。128ビット暗号化をサポートしないエンドポイントがない限り、弱い暗号化は使用しないでください。

デバッグモード

デバッグモードの有効化：このオプションで、PPTPログで生成されるデバッグ出力の量を制御します。接続で問題が発生し、クライアントパラメータのネゴシエーションに関する詳細な情報が必要である場合などに、このオプションを選択します。

16.3 L2TP over IPsec

L2TP（*Layer Two (2) Tunneling Protocol*の略称）とは、既存のネットワーク（通常はインターネット）を介して 2つのピア間でネットワークトラフィックをトンネリングするためのデータリンクレイヤ（OSI モードのレイヤ2）プロトコルであり、VPN とも呼びます。L2TP プロトコルには機密性が欠けるため、多くの場合は機密性、認証、完全性を提供するIPsec と組み合わせて使用します。これら2つのプロトコルの組み合わせを別名「L2TP over IPsec」と呼びます。L2TP over IPsecを使用すると、PPTP と同じ機能を提供しながら、暗号化されたIPsecトンネル経由のネットワークアクセスを個々のホストに提供することができます。

16.3.1 グローバル

*L2TP over IPsec > グローバル*タブでは、L2TPover IPsec経由のリモートアクセスをセットアップするための基本オプションを設定できます。

L2TP over IPsecを使用するには、次の手順に従ってください。

1. ***グローバル*タブで、L2TP over IPsecを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、*サーバ設定およびIPアドレス割り当て*エリアが編集可能になります。

2. **次の設定を行います。**
   インタフェース: L2TP VPNアクセスに使用するネットワークインタフェースを選択します。

   認証モード: 次の認証モードを選択できます。

- 事前共有鍵：事前共有鍵として使用されるパスワードを入力します。*事前共有鍵*方式では、通信を行う前に、通信当事者間で共有シークレットを交換します。通信のためには、シークレットを知っていることを両者が証明します。共有シークレットとは、L2TP用の暗号化アルゴリズムを使用してトラフィックを暗号化するために使用される安全なフレーズまたはパスワードです。セキュリティを高めるために、共有シークレットを強化する適切な手法をとる必要があります。共有シークレットのセキュリティは、パスワードの品質と、それをどれだけ安全に伝送するかにかかっています。一般的な言葉から成るパスワードは、辞書攻撃に対して非常に脆弱です。そのため、共有シークレットは非常に長くし、さまざまな文字、大文字、数字を組み合わせる必要があります。そのため、事前共有シークレットを使用する認証方式は、可能な限り証明書方式に切り替える必要があります。

  > 注 –iOSデバイスではPSK認証のみがサポートされているため、iOSデバイスへのアクセスを有効にするためには、*事前共有鍵*を選択する必要があります。

- **X.509 CA**チェック: X.509証明書により、参加者の多い大規模なVPNセットアップでの公開認証鍵の交換が容易になります。いわゆるCAがVPNエンドポイントの公開鍵を収集してチェックし、各メンバに対して証明書を発行します。証明書には、ピアのアイデンティティと公開鍵が含まれています。証明書はデジタル署名されているため、検出されずに他人が偽造証明書を発行することはできません。

  鍵交換中に証明書が交換され、ローカル保存されたCA公開鍵を使用して検証されます。続いて、公開鍵とプライベート鍵を使用してVPNエンドポイントの実際の認証が行われます。この認証モードを使用するためには、X.509証明書を選択します。

  X.509認証が機能するためには、*リモートアクセス* > *証明書管理* > *認証局 CA* タブで有効なCAを設定する必要があります。

IPアドレスの割り当て: IPアドレスは、事前に定義したIPアドレスプールから割り当てることも、DHCPサーバを使用して自動的に配布することもできます。

- プールネットワーク: デフォルトでは、IPアドレスの割当方法として*IPアドレスプール*が選択されており、*プールネットワーク*には事前定義済みの*VPNプール L2TP* ネットワーク定義が選択されています。*VPNプール L2TP* とは、プライベートインターネット用のIPアドレススペース`10.x.x.x`からクラスCサブネットを使用してランダムに生成されたネットワークです。これは、ユーザが接続元として専用のアドレスプールを持つことを保証するものであり、通常は一切変更する必要がありません。別のネットワークを使用したい場合は、*VPNプール L2TP* の定義を変更するか、ここでIPアドレスプールとして他のネットワークを割り当てます。ネットマスクは最低16までに制限

されいますので注意してください。

> 注 – L2TP VPNプールに対してプライベートIPアドレスを使用しており、インターネットへのアクセスにIPsecホストを許可したい場合、適切なマスカレーディングまたはNATルールをIPアドレスプールに用意する必要があります。

- **DHCP**サーバ: *DHCPサーバ*を選択する場合、DHCPサーバが接続に使用するネットワークインタフェースも指定する必要があります。DHCPサーバーはインタフェースに直接接続する必要はありません。ルータを介してもアクセスできます。ローカルDHCP サーバーはサポートされません。ここで選択した DHCP サーバーは、物理的に異なるシステム上で稼働している必要があります。

3. *適用*をクリックします。
   設定が保存されます。

   トグルスイッチが緑色に変わります。

設定をキャンセルするには、アンバー色のトグルスイッチをクリックします。

アクセス制御

認証要求先: L2TPリモートアクセスは、ローカル認証とRADIUS認証のみをサポートします。

- ローカル: *ローカル*を選択する場合、L2TPリモートアクセスを使用できるようにするユーザとユーザグループを指定してください。バックエンドのユーザグループをフィールドにドラッグすることはできません。ローカルユーザの場合、通常の方法でユーザを追加し、これらのユーザに対してL2TPを有効にします。ユーザーまたはグループを選択しない場合、L2TP リモートアクセスはオフになります。ユーザを追加する方法は、*定義とユーザ* > *ユーザとグループ*> *ユーザ*ページで説明しています。

  > 注 – 選択したユーザのユーザ名およびパスワードには、ASCII印字可能文字[1]だけが含まれています。

  > 注 – SSLVPN同様、ユーザポータルの *リモートアクセス*メニューにアクセスできるのは、*ユーザとグループ**UTM*ボックスで選択されたユーザと、ユーザ定義がに定義されているユーザのみです。認証モードに応じて、ユーザポータルへのログインに成功した認証ユーザには、IPsec事前共有鍵(認証モード*事前共有鍵*)または`PKCS#12`ファイル(認証モー

[1] http://en.wikipedia.org/wiki/ASCII#ASCII_printable_characters

ドX.509 CA チェック)ならびにインストール手順(SophosKnowledgebaseで提供)へのリンクが提供されます。

- **RADIUS**: *RADIUS*を選択すると、認証要求はRADIUSサーバに転送されます。L2TPモジュールは、NAS-IDとして、次の文字列をRADIUSサーバに送信します。`l2tp`。

クライアントとサーバ間で、認証アルゴリズムのネゴシエーションが自動的に行われます。ローカルユーザに対し、Sophos UTMは認証プロトコルMSCHAPv2をサポートしています。

RADIUSユーザに対し、Sophos UTMは次の認証プロトコルをサポートしています。

- MSCHAPv2
- MSCHAP
- CHAP

16.3.2 iOSデバイス

ユーザポータルでiOSデバイスユーザに対し自動L2TP over IPsec設定を提供することができます。

ただし、*グルーバル*タブの*ユーザーとグループ*ボックスに追加されたユーザーのみに対して、ユーザーポータルサイトに設定ファイルが表示されます。iOS デバイスのステータスはデフォルトで有効になっています。

コネクション名 : L2TP over IPsecコネクションを説明する名前を入力し、iOSデバイスのユーザがどのコネクションを確立しようとしているのか識別できるようにします。デフォルトの名前は、お客様の会社名の後にL2TP over IPsec プロトコルが続いたものになります。

注 – *コネクション名*はすべての iOS デバイス設定(PPTP、L2TP over IPsec、Cisco VPN Client)で一意である必要があります。

ホスト名 を上書 き: システムのホスト名をクライアントがパブリックに解決できない場合は、ここにサーバのホスト名を入力して、これによって*システムのDNSホスト名*の前の*DynDNSホスト名*の内部プリファレンスを上書きします。

iOS デバイスの自動設定を無効にするには、トグルスイッチをクリックします。

トグルスイッチはグレーになります。

16.3.3 デバッグ

IKEデバッグ

*IKEデバッグ*セクションでIKEデバッグオプションを設定できます。どのタイプのIKEメッセージまたは通信についてデバッグ出力を作成するかはチェックボックスで選択します。

注 – *IKEデバッグ*セクションは、*サイト間VPN IPsec*、*リモートアクセスIPsec*、*L2TP over IPsec*、および*Cisco VPN クライアント*メニューの *デバッグ*タブで同じものが使用されています。

以下のフラグをログできます。

- *コントロールフロー*:IKEステートのコントロールメッセージを表示します。
- *送信パケット*:送信IKEメッセージのコンテンツを表示します。
- *受信パケット*:受信IKEメッセージのコンテンツを表示します。
- *カーネルメッセージ*:カーネルとの通信メッセージを表示します。
- *冗長化*:その他のHA ノードとの通信を表示します。

L2TPデバッグ

*デバッグモードを有効にする*を選択すると、*IPsec VPN*ログファイルに、L2TPまたはPPP接続ネゴシエーションに関する多くの情報が含まれるようになります。

16.4 IPsec

*IPsec*とは、すべてのIPパケットを暗号化または認証すること(あるいはその両方)によってIP(*インターネットプロトコル*)通信のセキュリティを維持するための標準です。

IPsec標準は、次の2つのサービスモードと2つのプロトコルを定義しています。

- トランスポートモード
- トンネルモード
- *AH*(*認証ヘッダ*)認証プロトコル
- *ESP*(*カプセル化セキュリティペイロード*)暗号化(および認証)プロトコル

IPsecには、SA(*セキュリティアソシエーション*)と鍵配布を手動および自動で管理するための方法も用意されています。これらの特徴は、DOI (*解釈ドメイン*) で一元管理されています。

IPsecモード

IPsecは、トランスポートモードまたはトンネルモードで機能します。原則的に、ホスト間接続ではどちらのモードも使用できます。ただし、いずれかのエンドポイントがセキュリティゲートウェイである場合、トンネルモードを使用する必要があります。この UTM での IPsec VPN 接続では、常にトンネルモードが使用されます。

トランスポートモードでは、元のIPパケットは他のパケットにカプセル化されません。元のIPヘッダは維持され、パケットの残りの部分は平文のまま(AH)またはカプセル化されて(ESP)送信されます。パケット全体をAHで認証することも、ESPでペイロードをカプセル化して認証することもできます。いずれの場合も、元のヘッダは平文としてWAN経由で送信されます。

トンネルモードでは、パケットヘッダとペイロードの全体が新しいIPパケットにカプセル化されます。IPヘッダがIPパケットに追加され、宛先アドレスは受信側トンネルエンドポイントに設定されます。カプセル化パケットのIPアドレスは変更なしで維持されます。続いて、元のパケットがAHで認証されるか、ESPでカプセル化されて認証されます。

IPsecプロトコル

IPsecでは、IPレベルで安全に通信するために2つのプロトコルを使用します。

- **AH** 認証ヘッダ :パケット送信者を認証し、パケットデータの完全性を保証するためのプロトコル。
- **ESP** カプセル化セキュリティペイロード :パケット全体を暗号化し、そのコンテンツを認証するためのプロトコル。

AH 認証ヘッダ プロトコルは、パケットデータの信頼性と完全性をチェックします。さらに、送信者と受信者のIPアドレスが送信中に変更されていないことをチェックします。パケットは、*ハッシュベースのメッセージ認証コード*(HMAC)と鍵を使用して作成されたチェックサムを使用して認証されます。次のいずれかのハッシュアルゴリズムが使用されます。

- **MD5** メッセージダイジェスト、バージョン**5** :このアルゴリズムでは、任意のサイズのメッセージから128ビットのチェックサムが生成されます。このチェックサムはメッセージの指紋のようなもので、メッセージが変更されるとチェックサムも変わります。このハッシュ値は、デジタル署名またはメッセージダイジェストとも呼ばれます。
- **SHA-1** セキュアハッシュ :このアルゴリズムではMD5と類似したハッシュが生成されますが、SHA-1ハッシュは長さが160ビットです。SHA-1は鍵がMD5より長いため、MD5より強力なセキュリティが実現します。

MD5と比較すると、SHA-1ハッシュは計算が難しく、生成に必要なCPU時間はより長くなります。もちろん、計算速度は、プロセッサの処理速度とSophos UTMで使用されるIPsec VPN 接続の数に依存します。

ESP *カプセル化セキュリティペイロード* プロトコルには、暗号化以外に、送信者を認証し、パケットコンテンツを検証する機能もあります。トンネルモードで ESP を使用すると、IP パケット全体(ヘッダとペイロード)が暗号化されます。ここで、暗号化されていないIPヘッダとESPヘッダがカプセル化するパケットに追加されます。新しいIPヘッダには、受信側ゲートウェイと送信側ゲートウェイのアドレスが含まれています。これらのIPアドレスは、VPNトンネルのアドレスです。

暗号化付きのESPでは、通常次のアルゴリズムが使用されます。

- 3DES(トリプルデータ暗号化標準)
- AES(高度暗号化標準)

これらのうち、AESが最も安全です。AESで使用可能な鍵の有効長は128ビット、192ビット、256ビットです。Sophos UTMは、多数の暗号化アルゴリズムをサポートしています。認証にはMD5またはSHA-1アルゴリズムを使用できます。

NAT トラバーサル NAT-T

NATトラバーサルとは、NATデバイスを使用するTCP/IPネットワーク内のホスト間で接続を確立するための技術です。この接続は、ESPパケットのUDPカプセル化を使用して、NATデバイス経由でIPsecトンネルを確立することによって実現します。UDPカプセル化は、IPsecピア間でNATが検出された場合のみに使用されます。検出されなかった場合は、通常のESPパケットが使用されます。

NATトラバーサルにより、ゲートウェイまたはロードウォリアをNATルータの背後に配置しながら、IPsecトンネルを確立できるようになります。この機能を使用する場合、両方のIPsecピアでNATトラバーサルがサポートされている必要があります。ネゴシエーションは自動的に行われます。NATデバイスでIPseパススルーがオフになっていることを確認してください。オンになっていると、NATトラバーサルの使用に支障が出る可能性があります。

ロードウォリアでNATトラバーサルを使用したい場合、WebAdmin内の対応ユーザオブジェクトにスタティック(静的)なリモートアクセスIPアドレス(RASアドレス)が設定されている必要があります(WebAdminの *ユーザ*ページの *スタティックリモートアクセスIPを使用*も参照してください)。

データ未送信時に確立されたトンネルが期限切れになることを防ぐために、NATトラバーサルのkeep-alive信号がデフォルトで60秒間隔で送信されます。keep-aliveメッセージは、NATルータがセッションに関連するステート情報を維持しており、トンネルが開いたままであることを確認するために送信されます。

TOS

「サービスタイプ」ビット(TOSビット)は、IPヘッダにあるいくつかの4ビットフラグです。これらのビットは、どのタイプのサービス品質が必要であるかを転送アプリケーションがネットワークに伝えることを許可するため、*サービススタイプ*ビットと呼ばれています。

Sophos UTMへの IPsec 導入では、TOS の値は常にコピーされます。

16.4.1 コネクション

*IPsec > コネクション*タブでは、IPsecコネクションを作成し、編集することができます。

IPsecコネクションを作成するには、次の手順に従います。

1. ***コネクション*タブで*新規IPsec リモートアクセスルール*をクリックします。**
   *IPsec リモートアクセスルールの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前: このコネクションを説明する名前を入力してください。

   インタフェース: IPsecトンネルのローカルエンドポイントとして使用されるインタフェースの名前を選択します。

   ローカルネットワーク: VPNトンネル経由でアクセス可能にするローカルネットワークを選択または追加します。定義を追加する方法は、*定義とユーザ > ネットワーク定義 > ネットワーク定義*ページで説明しています。

   仮想IPプール: クライアントにスタティックIPアドレスが定義されていない場合、クライアントはこのIPアドレスプールに割り当てられたIPアドレスを取得します。デフォルトプールは*VPNプール (IPsec)* であり、プライベートIPスペース`10.242.4.0/24`から成ります。ただし、他のIPアドレスプールを選択または作成することもできます。ネットマスクは最低16に制限されていますので注意してください。定義を追加する方法は、*定義とユーザ > ネットワーク定義 > ネットワーク定義*ページで説明しています。

   ポリシ: このIPsecコネクションのIPsecポリシを選択します。IPsecポリシは、*リモートアクセス > IPsec > ポリシ*タブで定義できます。

   認証タイプ: このリモートゲートウェイ定義の認証タイプを選択します。次のタイプを使用できます。

- **事前共有鍵**:*事前共有鍵*(PSK)による認証では、秘密のパスワードを鍵として使用します。これらのパスワードは、接続を確立する前にエンドポイントに配布する必要があります。新しいVPNトンネルが確立されると、両端で、相手側が秘密のパスワードを知っていることのチェックが行われます。PSKのセキュリティは、使用するパスワードの品質に依存します。一般的な言葉や成句では、辞書攻撃に対して脆弱です。常時の、または長期的なIPsecコネクションでは、パスワードの代わりに証明書を使用すべきです。

- **X.509証明書**:X.509証明書による認証方式では、公開鍵と秘密鍵を使用します。X.509証明書には、公開鍵と、鍵の所有者を特定する情報が含まれています。このような証明書は、信頼される*認証局*(CA)によって署名され、発行されたものです。選択後、このIPsec接続の使用を許可するユーザを指定します。*自動ファイアウォールルール*チェックボックスにチェックを入れた場合を除き、適切なファイアウォールルールを*ネットワークプロテクション*メニューに手動で指定する必要があります。

  注 – ユーザポータルにアクセスできるのは、*許可ユーザ*ボックスで選択されており、UTMにユーザ定義が存在するユーザのみです。ユーザポータルへのログインに成功した認証されたユーザには、*SophosIPsecクライアント*(SIC)、設定ファイル、`PKCS#12`ファイル、インストール手順(SophosKnowledgebaseで提供)へのリンクが提供されます。

- **CA DN照合**:この認証タイプでは、CA証明書のDN *識別名* の照合を使用して、VPNエンドポイントの鍵を検証します。選択した場合、*認証局*を1つ選択し、リモートアクセスクライアントのDNと一致する*DNマスク*を選択します。ここで、*ピアサブネット範囲*を選択または追加します。クライアントは、いずれかの証明書がDNマスクと一致しなければ接続が許可されません。

XAUTHの有効化(オプション):設定されたバックエンドに対するユーザ認証が必要である場合は、拡張認証を有効にする必要があります。

自動ファイアウォールルール(オプション):このオプションは、認証タイプ*X.509証明書*のみで使用可能です。このオプションを選択すると、この接続のトラフィックを許可するファイアウォールルールを自動的に追加することができます。ルールは、接続が有効になるとすぐに追加され、接続が切断されると削除されます。

コメント(オプション):説明などの情報を追加します。

3. ***保存*をクリックします。**
   新しいリモートアクセスルールが*コネクション*リストに表示されます。

リモートアクセスルールを編集または削除するには、対応するボタンをクリックします。

16.4.2 ポリシー

*リモートアクセス > IPsec > ポリシ*タブでは、IPsecコネクションのパラメータをカスタマイズし、ポリシに統合することができます。IPsecポリシは、IPsec接続のIKE(インターネット鍵交換)とIPsecプロポーザルパラメータを定義します。それぞれのIPsec接続にはIPsecポリシが必要です。

注 – Sophos UTM は、IKE フェーズ 1 のメインモードのみをサポートしています。アグレッシブモードはサポートされていません。

IPsecポリシを作成するには、以下の手順に従います。

1. ***ポリシ*タブで、*新規IPsecポリシ*をクリックします。**
   *IPsecポリシの追加*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:このポリシを説明する名前を入力します。

   IKE暗号化 *アルゴリズム*:暗号化アルゴリズムでは、IKEメッセージの暗号化に使用するアルゴリズムを指定します。以下のアルゴリズムがサポートされています。

   - *DES*(56ビット)
   - *3DES*(168ビット)
   - *AES 128*(128ビット)
   - *AES 192*(192ビット)
   - *AES 256*(256ビット)
   - *Blowfish*(128ビット)
   - *Twofish*(128ビット)
   - *Serpent*(128ビット)

   セキュリティに関する注記 – 弱いアルゴリズムであり、潜在的脆弱性を表しているため、DESを使うことを強く推奨します。

   IKE認証 *アルゴリズム* 認証アルゴリズムでは、IKEメッセージの完全性チェックに使用するアルゴリズムを指定します。以下のアルゴリズムがサポートされています。

- *MD5*（128ビット）
- *SHA1*（160ビット）
- *SHA2 256*（256ビット）
- *SHA2 384*（384ビット）
- *SHA2 512*（512ビット）

IKE SA *ライフタイム* この値には、IKE SA（セキュリティアソシエーション）が有効な期間（つまり次の鍵更新を行うタイミング）を秒単位で指定します。有効な値は60秒～28800秒（8時間）です。デフォルト値は7800秒です。

IKE DH*グループ* 接続をネゴシエートする際は、通信するパーティはデータの暗号化に使用する実際の鍵についても取り決めます。IKEはセッション鍵を生成するために、ランダムデータを利用する*Diffie-Hellman*（DH）アルゴリズムを使用します。ランダムデータの生成はプールビットに基づいて行われます。基本的にはIKEグループがプールビット数を知らせます。プールビット数が多いほど、ランダムな数字が大きくなります。数字が大きいほど、Diffie-Hellmanアルゴリズムの解読は難しくなります。結果として、プールビット数が多ければ安全ですが、CPUリソースの消費量も増えます。現在は以下のDiffie-Hellmanグループがサポートされています。

- *グループ1 : MODP 768*
- *グループ2 : MODP 1024*
- *グループ5 : MODP 1536*
- *グループ14 : MODP 2048*
- *グループ15 : MODP 3072*
- *グループ16 : MODP 4096*

セキュリティに関する注記 - グループ1（MODP 768）は弱く、相互運用性の理由からのみサポートされています。潜在的脆弱性を表しているため、それを使うことを強く推奨します。

IPsec暗号化 *アルゴリズム*IKEの場合と同じ暗号化アルゴリズム。さらに、以下のエントリもあります。

- *暗号化なし null*
- *AES 128 CTR*（128ビット）

- *AES 192 CTR*（192ビット）
- *AES 256 CTR*（256ビット）
- *AES 128 GCM 96 ビット*
- *AES 192 GCM 96 ビット*
- *AES 256 GCM 96 ビット*
- *AES 128 GCM 128 ビット*
- *AES 192 GCM 128 ビット*
- *AES 256 GCM 128 ビット*

セキュリティに関する注記 – これは潜在的脆弱性を表しているため、暗号化を使用しないか、DESを使用することを推奨いたします。

IPsec認証 *アルゴリズム*：IKEの場合と同じ認証アルゴリズム。さらに、以下のアルゴリズムもあります。

- *SHA2 256*（96ビット）
- *SHA2 384*（96ビット）
- *SHA2 512*（96ビット）

これらは、RFC 4868に準拠しないトンネルエンドポイント、たとえばV8以前のUTM（例、ASGバージョンなど）への対応のために用意されています。そのため、96ビットより長い切り捨てられたチェックサムをサポートしません。

IPsec SA *ライフタイム*：この値には、IPsec SAが有効な期間（つまり次の鍵更新を行うタイミング）を秒単位で指定します。有効な値は60秒～86400秒（1日）です。デフォルト値は3600秒です。

IPsec PFS*グループ*：*Perfect Forward Secrecy*（PFS）という概念では、セッション鍵を使用できなくなった場合に、この特定セッションのデータにのみアクセスを許可します。PFSが存在するには、IPsec SAの保護に使用される鍵は、IKE SAの鍵を取得するために使用されるランダム鍵作成用のマテリアルから派生したものではないことが必要です。その場合、PFSは2回目のDiffie-Hellman鍵交換を開始し、IPsec接続に対して選択されたDHグループが新たにランダム生成された鍵を取得することを提案します。サポートされているDiffie-HellmanグループはIKEの場合と同じです。

PFSを有効にすると安全性が高まりますが、交換にさらに時間がかかるようになります。低速なハードウェアではPFSは使用しないことをお勧めします。

注 - PFSはすべてのベンダーとの完全な相互運用性はありません。ネゴシエーション時に問題が発生した場合は、PFSを無効にしてください。

厳密ポリシー:IPsecゲートウェイが暗号化アルゴリズムおよびその強度について提案を行うと、IPsecポリシがそれに対応していない場合でも、受信側ゲートウェイがこの提案を受け入れる場合があります。このオプションを選択すると、指定したパラメータを厳密にそのとおり使用することについてリモートエンドポイントが合意しないときは、IPsec接続は確立されません。UTMのIPsecポリシがAES-256暗号化を必要とする際に、SSH Sentinelを使用するロードウォリアがAES-128を使用して接続しようとすると、厳格なポリシオプションが有効である場合は、接続は拒否されます。

注 – 圧縮の設定は*厳格なポリシ*を介しては施行されません。

圧縮:このオプションでは、*IPペイロード圧縮プロトコル*(IPComp)によってIPパケットを暗号化の前に圧縮するかどうかを指定します。IPCompはIPパケットを圧縮してそのサイズを縮小し、通信ホストまたはゲートウェイのペア間の全体的な通信パフォーマンスを向上させます。デフォルトでは圧縮はオフになっています。

コメント(オプション):説明などの情報を追加します。

3. ***保存*をクリックします。**
   新しいポリシが*ポリシ*リストに表示されます。

ポリシーを編集または削除するには、対応するボタンをクリックします。

16.4.3 詳細

*リモートアクセス > IPsec > 詳細*タブで、IPsecVPNの詳細オプションを設定できます。希望の認証タイプに応じて、ローカル証明書(X.509認証の場合)やローカルRSA鍵(RSA認証の場合)などを定義可能です。この設定は熟練ユーザのみが行ってください。

ローカルX.509証明書

X.509認証では、証明書を使用してVPNエンドポイントの公開鍵を検証します。この認証タイプを使用する場合は、*ローカルX.509証明書*エリアのドロップダウンリストからローカル証明書を選択す

る必要があります。選択した鍵/証明書は、X.509認証が選択された場合のリモートピアへのゲートウェイの認証に使用されます。

適切な秘密鍵がある証明書のみ選択できます。他の証明書はこのドロップダウンリストでは利用できません。

選択できる証明書がない場合、新しい証明書を作成するか、またはアップロード機能を使用してインポートして、*証明書管理*メニューで追加する必要があります。

証明書を選択したら、秘密鍵を保護するパスフレーズを入力します。パスフレーズは保存プロセスで確認され、パスフレーズが暗号化鍵と一致しない場合はエラーメッセージが表示されます。

アクティブな鍵/証明書を選択すると、それは*ローカルX.509証明書*エリアに表示されます。

デッドピア検出 DPD

デッドピア検出 **(DPD)** を使用：デッドピア検出オプションを使用して、リモートVPNゲートウェイあるいはクライアントに接続できない場合は接続を自動的に終了します。スタティックエンドポイントとの接続では、トンネルは自動的に再ネゴシエートされます。ダイナミックエンドポイントとの接続では、リモート側でトンネルの再ネゴシエートを行うことが必要です。通常はこのオプションを常に有効にしておくほうが安全です。IPsecピアはリモート側がデッドピア検出をサポートするかどうかを自動的に判断し、必要に応じて通常モードにフォールバックします。

NATトラバーサル NAT-T

NAT トラバーサルを使用：このオプションを選択すると、IPsecトラフィックは、*ネットワークアドレス変換*（NAT）を使用するアップストリームシステムを通過できるようになります。さらに、NATトラバーサルのキープアライブ間隔を定義できます。設定を保存するには*適用*をクリックします。

CRL処理

証明書のプロバイダが、まだ有効な証明書に与えられる承認を取り消す場合があるかもしれません。たとえば、証明書の受取人が不正なデータ（名前など）を使ってそれを不正に取得したことが判明した場合や、証明書に埋め込まれた公開鍵の一部である秘密鍵を攻撃者が入手した場合は、証明書が失効します。そのような場合に備えて、いわゆる*証明書失効リスト*（CRL）が使用されます。CRLには通常、依然として有効期間は残っているものの無効とされた証明書のシリアル番号が含まれています。

これらの有効期限が切れると、証明書は無効になり、ブロックリストから削除されます。

自動*フェッチ*：この機能は、HTTP、Anonymous（匿名）FTP、またはLDAPバージョン3を介しパートナー証明書で定義されたURLを通してCRLを要求します。有効期限が切れたら、要求によってCRLをダウンロードし、保存して更新できます。この機能を、ポート80または443を経由せずに使用

する場合は、適切なファイアウォールルールを設定して、CRL配布サーバにアクセスできるようにしてください。

厳密ポリシー：このオプションを有効にすると、対応するCRLのないパートナー証明書は拒否されます。

PSKプローブ

応答のみモードを使用したIPsec接続では、それぞれのIPsec接続に対して別々の事前共有鍵（PSK）を使用することを選択できます。

PSKプローブの有効化：このチェックボックスにチェックを入れて、このオプションを有効にします。この設定は、L2TP-over-IPsec、リモートアクセスIPsec、VPN IPsecの各接続に影響を与えます。

16.4.4 デバッグ

IKEデバッグ

*IKEデバッグ*セクションでIKEデバッグオプションを設定できます。どのタイプのIKEメッセージまたは通信についてデバッグ出力を作成するかはチェックボックスで選択します。

注 – *IKEデバッグ*セクションは、*サイト間VPN IPsec*、*リモートアクセスIPsec*、*L2TP over IPsec*、および*Cisco VPN クライアント*メニューの*デバッグ*タブで同じものが使用されています。

以下のフラグをログできます。

- コントロールフロー：IKEステートのコントロールメッセージを表示します。
- 送信パケット：送信IKEメッセージのコンテンツを表示します。
- 受信パケット：受信IKEメッセージのコンテンツを表示します。
- カーネルメッセージ：カーネルとの通信メッセージを表示します。
- 冗長化：その他のHAノードとの通信を表示します。

16.5 HTML5 VPNポータル

HTML5 VPNポータル機能を使用すると、外部ネットワークのユーザは、プラグインをインストールしなくても、ブラウザのみをクライアントとして使用して、あらかじめ設定されているコネクションタイプで内部リソースにアクセスすることができます。このためには、ユーザーはUTMのユーザーポータルにログインする必要があります。このポータルの*HTML5 VPNポータル*タブには、このユーザーが

使用できる全コネクションのリストが表示されます。*接続*ボタンをクリックすると、定義されている内部リソースへの接続が開始されます。管理者は、許可ユーザー、コネクションタイプ、その他の設定を指定して、事前にこれらのコネクションを作成する必要があります。内部リソースへのアクセスには、リモートデスクトップにアクセスするためのリモートデスクトッププロトコル(RDP)か仮想ネットワークコンピューティング(VNC)、Webアプリケーション(HTTP/HTTPS)を使用するためのブラウザ、ターミナルセッション用のTelnet/セキュアシェル(SSH)など、各種のコネクションタイプを使用できます。ただし、HTML5 VPNポータルは、コンテンツのダウンロードを許可しません。例、HTTP経由でのユーザのローカルコンピュータへのダウンロード。

この機能を使用すると、それ自体ではマルチユーザーアクセスをサポートしない内部リソース(スイッチのようなネットワークハードウェアなど)への複数ユーザーのアクセスを許可したり、システムまたはネットワーク全体へのアクセスを許可するのではなく、1つのサービスのみに絞った詳細なアクセス管理を簡単に行うことができます。

例:

- 電話システムを保守する電話サービス会社にアクセスを提供。
- イントラネットなど、特定の内部Webサイトへのアクセスを提供。

注 – ブラウザは HTML5 に準拠したものである必要があります。次のブラウザはHTML5 VPN機能をサポートしています: Firefox 6.0以降、Internet Explorer 10以降、Chrome、Safari 5以降、(MACのみ)。

注 – 専用セッションで複数のユーザを指定することはできません。

16.5.1 グローバル

*リモートアクセス > HTML5 VPN ポータル > グローバル*タブでは、HTML5 VPNポータルを有効化し、各VPNポータルコネクションを管理できます。接続の数は、100までに制限されています。許可されたユーザの場合、ユーザポータルの*HTML5 VPN ポータル*タブで有効な接続を使用できます。

HTML5 VPNポータルを有効化して、新規HTML5 VPNコネクションを作成するには、次の手順に従います。

1. **HTML5 VPNポータルを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチが緑色に変わり、ページ内の要素が編集可能になります。許可されているユーザには、有効にされている既存の全コネクションがユーザポータルに表示されます。

2. *新規* ***HTML5 VPN*** *ポータルコネクション***ボタンをクリックします。**
   *HTML5 VPN ポータルコネクションの追加*ダイアログボックスが開きます。

3. **次の設定を行います。**
   名前 : このコネクションを説明する名前を入力してください。

   コネクションタイプ: コネクションタイプを選択します。選択したコネクションタイプによっては、異なるパラメータが表示されます。次のタイプを使用できます。

   - *リモートデスクトップ*: Windowsホストでリモートデスクトップセッションを開始する場合などの、リモートデスクトッププロトコル(RDP)を使用したリモートアクセス。
   - **Webapp (HTTP)**: HTTPを使用したWebアプリケーションへのブラウザベースのアクセス。
   - **Webapp (HTTPS)**: HTTPSを使用したWebアプリケーションへのブラウザベースのアクセス。

     注 – **HTTP/HTTPS** 接続に使用される**URL**は、このコネクションの*宛先*、*ポート*、およびパスオプションから構成されます。Webアプリケーションは、Mozilla Firefox (バージョン6.0以降)に対応しなければなりません。

   - **Telnet**: スイッチやプリンタにアクセスを提供する場合などの、Telnetプロトコルを使用したターミナルアクセス。
   - **SSH**: SSHを使用したターミナルアクセス。
   - **VNC**: Linux/Unixホストのリモートデスクトップを開く場合などの、仮想ネットワークコンピューティング(VNC)を使用したリモートアクセス。

     注 – 現在は、VNC クラシック認証 (パスワードのみ) がサポートされています。サーバがそれに応じてセットアップされていることを確認してください。

   宛先 : 許可されたユーザが接続できるホストを選択または追加します。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

   注 – 選択した宛先ホストが自己署名証明書を提供する場合、証明書のCN(一般名)が宛先ホスト名と一致することを確認してください。一致しない場合は、ポータルのブラウザに証明書警告が出ます。たとえば、DNSホストとして*www.mydomain.com*を使用する場合、自己署名証明書にこの名前が含まれることを確認してください。DNSホストの代わりにホ

ストを使用する場合、ホストのIPアドレスが*SAN (Subject Alternative Name)*として自己署名証明書に含まれていることを確認してください。

パス（*Webapp*のコネクションタイプのみ）：許可されたユーザが接続できるパスを入力します。

ユーザ名（*SSH*のコネクションタイプのみ）：ユーザが接続に使用するユーザ名を入力します。

自動ログイン/自動ログイン 基本認証 ：有効にすると、ユーザは認証データを知らなくてもログインできます。この場合は、管理者が認証データを提供する必要があります。表示されるオプションは選択したコネクションタイプに依存します。

- ユーザ名：ユーザが接続に使用するユーザ名を入力します。
- パスワード：ユーザが接続に使用するパスワードを入力します。

> 注 – 接続タイプ*Telnet*を使用する場合、セキュリティ上の理由から、自動ログインが機能するには、Telnetサーバから送信されるバナーの長さが4096文字（パスワードプロンプトを含む）を超えない場合だけです。バナーが長すぎると、自動ログインは失敗します。この場合、バナーの長さを短縮するか、手動ログインに切り替えます。

- 認証方式（*SSH*のコネクションタイプのみ）：SSH認証方式を選択します。選択したユーザ名に対する*パスワード*を提供するか、SSH接続の*SSH秘密鍵*を追加できます。

SSL ホスト証明書（*HTTPS*のコネクションタイプのみ）：宛先ホストを識別するSSLホストのセキュリティ証明書を追加します。

- **SSL**証明書：*フェッチ*ボタンをクリックして、選択した宛先ホストの証明書を自動的に追加します。

ホスト公開鍵（SSHのコネクションタイプのみ）：*SSH*ホストの公開鍵を追加します。

- **SSH**公開鍵：*フェッチ*ボタンをクリックして、選択した宛先ホストのSSH公開鍵を自動的に取得します。

許可ユーザ ユーザポータル ：VPNポータル接続の使用を許可するユーザまたはグループを選択するか、新しいユーザを追加します。デフォルトでは、同時に接続を使用できるのは1ユーザだけです。ユーザに同時にセッションを共有させたい場合は、*詳細*セクションで*共有*

*セッション*チェックボックスを選択します。ユーザを追加する方法は、*定義とユーザ* > *ユーザとグループ* > *ユーザ*ページで説明しています。

注 – バックエンドメンバシップのグループを追加する場合、そのグループがユーザポータルについても許可されていることを確認してください。*マネジメント* > *ユーザーポータル* > *グローバル*タブ、から選択するか、*全てのユーザーを許可* か *特定のユーザーのみ*もしくは明確にグループを追加。ユーザポータルに対して個別のグループメンバだけを許可する場合、グループに対して許可された接続は提供されません。

コメント(オプション):説明などの情報を追加します。

4. **次の詳細設定を任意で行います。**
ポート:コネクションのポート番号を入力します。デフォルトでは、選択したコネクションタイプの標準ポートが選択されます。

プロトコルセキュリティ(接続タイプ *リモートデスクトップ*の場合のみ):リモートデスクトップセッションのセキュリティのプロトコルを選択します。RDP、TLS、NLA (ネットワークレベル認証)のいずれかを選択できます。設定は、サーバの設定と適合している必要があります。NLAでは、*自動ログイン*以上を有効にする必要があります。

共有セッション:このオプションを選択すると、ユーザが同時にセッションを使用して、同じ画面を表示することを許可します。

外部リソースを許可 (接続タイプ*Webapp*の場合のみ):この接続でアクセスできる追加リソースを入力します。たとえば画像またはその他のリソースがWebページ自体と異なるサーバに保存される場合、これが便利です。選択したポートまたはネットワークで、ポート80および443が許可されます。

5. ***保存*をクリックします。**
新しいコネクションが *コネクション*リストに表示されます。

6. **コネクションを有効にします。**
トグルスイッチをクリックして、接続を有効にします。

許可されたユーザがコネクションを使用できるようになります。これは、ユーザポータルの*HTML5 VPN ポータル*タブに表示されます。

接続を編集または削除するには、対応するボタンをクリックします。

16.6 Cisco VPNクライアント

Sophos UTMは、Cisco VPNクライアント経由のIPsecリモートアクセスをサポートします。Cisco VPNクライアントは、Cisco Systems の提供する実行可能形式プログラムです。これを使用すると、コンピュータのセキュリティを維持しながら VPN (*バーチャルプライベートネットワーク*) にリモート接続することができます。

16.6.1 グローバル

リモートアクセス > *Cisco VPN クライアント* > *グローバル*タブでは、Cisco VPNクライアント経由のリモートアクセスをセットアップするための基本オプションを設定することができます。

Sophos UTMを設定してCisco VPNクライアント接続が許可されるようにするには、次の手順に従ってください。

1. ***グローバル*タブで、Cisco VPNクライアントを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、*サーバ設定*エリアが編集可能になります。

2. **次の設定を行います。**
   インタフェース: Cisco VPNクライアント接続に使用するインタフェースを選択します。

   サーバ証明書 : サーバがクライアントに対して自らの身元を証明するために使用する証明書を選択します。

   プールネットワーク: 接続クライアントに仮想ネットワークアドレスを割り当てるために、仮想ネットワークアドレスを選択するためのネットワークプールを選択します。デフォルトで*VPN プール (Cisco)* が選択されています。

   ローカルネットワーク: VPNトンネル経由でアクセス可能にするローカルネットワークを選択または追加します。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

   ユーザとグループ: Cisco VPNクライアント経由でUTMに接続することが許可されるユーザやユーザグループを選択するか、ユーザを追加します。ユーザを追加する方法は、*定義とユーザ* > *ユーザとグループ* > *ユーザ*ページで説明しています。

自動ファイアウォールルール（オプション）:このオプションを選択すると、この接続のトラフィックを許可するファイアウォールルールを自動的に追加することができます。ルールは、接続が有効になるとすぐに追加され、接続が切断されると削除されます。

3. ***適用*をクリックします。**
設定が保存されます。

トグルスイッチが緑色に変わります。

ライブログ

IPsec IKEデーモンログの接続ログを追跡するには、ライブログを使用します。ライブログには、接続の確立、維持、終了に関する情報が表示されます。

16.6.2 iOSデバイス

ユーザポータルでiOSデバイスに対しCisco IPsecの自動設定を提供することができます。

ただし、*グルーバル*タブの *ユーザーとグループ*ボックスに追加されたユーザーのみに対して、ユーザーポータルサイトに設定ファイルが表示されます。iOS デバイスのステータスはデフォルトで有効になっています。

コネクション名：Cisco IPsecコネクションを説明する名前を入力し、iOSデバイスのユーザがどのコネクションを確立しようとしているのか識別できるようにします。デフォルトの名前は、お客様の会社名の後に Cisco IPsec プロトコルが続いたものになります。

> **注 –** *コネクション名*はすべての iOS デバイス設定（PPTP、L2TP over IPsec、Cisco VPN Client）で一意である必要があります。

ホスト名を上書き:システムのホスト名をクライアントがパブリックに解決できない場合は、ここにサーバのホスト名を入力して、これによって *システムのDNSホスト名* の前の*DynDNSホスト名*の内部プリファレンスを上書きします。

*オンデマンドで***VPN** *コネクションを確立する*:ボックスにリストされているホスト名またはいずれかのドメインとロケーションが一致したときにVPN接続を自動的に開始するには、このオプションを選択します。

- *ドメインまたはホストと一致*：オンデマンドでVPN接続を確立させたいドメインまたはホスト名を入力します。これは、たとえばローカルのイントラネットなどになります。

- **DNSルックアップ失敗時のみ確立**：デフォルトでは、VPN接続が確立されるのは、DNS ルックアップが失敗した後だけです。選択を解除すると、ホスト名が解決されたか否かに関わらず、VPN接続が確立されます。

接続するiOSデバイスが、*グローバル*タブに指定したサーバ証明書に表示されます。iOSデバイスは、この証明書のVPN IDがサーバのホスト名と一致しているかチェックし、異なる場合には接続を拒否します。サーバ証明書でVPN IDタイプに*識別名*を使用している場合、代わりに*一般名*フィールドが使用されます。サーバ証明書がこれらの制約を満たしていることを確認する必要があります。

iOS デバイスの自動設定を無効にするには、トグルスイッチをクリックします。

トグルスイッチはグレーになります。

16.6.3 デバッグ

IKEデバッグ

*IKEデバッグ*セクションでIKEデバッグオプションを設定できます。どのタイプのIKEメッセージまたは通信についてデバッグ出力を作成するかはチェックボックスで選択します。

注 – *IKEデバッグ*セクションは、*サイト間VPN IPsec*、*リモートアクセスIPsec*、*L2TP over IPsec*、および*Cisco VPN クライアント*メニューの*デバッグ*タブで同じものが使用されています。

以下のフラグをログできます。

- コントロールフロー：IKEステートのコントロールメッセージを表示します。
- 送信パケット：送信IKEメッセージのコンテンツを表示します。
- 受信パケット：受信IKEメッセージのコンテンツを表示します。
- カーネルメッセージ：カーネルとの通信メッセージを表示します。
- 冗長化：その他のHA ノードとの通信を表示します。

16.7 詳細

*リモートアクセス > 詳細*ページでは、リモートアクセスクライアントの詳細設定を行うことができます。ここで入力するDNSサーバとWINSサーバのIPアドレスは、ゲートウェイへの接続の確立時にリ

モートアクセスクライアントを使用するために提供され、これによってドメインの完全な名前解決が実現します。

DNSサーバ: 組織のDNSサーバを最大2台指定します。

WINSサーバ: 組織のWINSサーバを最大2台指定します。 *Windowsインターネットネーミングサービス* とは、マイクロソフトがWindows OSに実装したNBNS *NetBIOSネームサーバ* です。DNSがドメイン名を対象にしているように、WINSはNetBIOS名を対象にしてホスト名とIPアドレスを一元的にマッピングします。

ドメイン名 : *完全修飾ドメイン名*（FQDN）として、UTMのホスト名を入力します。完全修飾ドメイン名とは、DNSツリー階層でのノードの絶対位置を指定する明瞭なドメイン名です（`utm.example.com`など）。ホスト名には英数字、ドット、およびハイフンを使用できます。ホスト名の末尾には`com`、`org`、`de`などの特殊な識別子を使用する必要があります。ホスト名は、通知メッセージでUTMを識別するために使用されます。

> 注 - PPTPおよびL2TP over IPsecの場合、ドメイン名は自動的に配信できず、クライアント側で設定する必要があります。
> *Cisco VPNクライアント*を使用するiOSデバイスでは、上で指定したDNSサーバが指定ドメインに属するホストの解決にのみ使用されます。

16.8 証明書管理

*サイト間VPN > 証明書管理*メニューと*リモートアクセス > 証明書管理*メニューには、同じ設定オプションが含まれています。これらの設定オプションを使用すると、Sophos UTMのすべての証明書関連オプションを管理することができます。中でも、X.509証明書の作成またはインポートや、*証明書失効リスト*（CRL）のアップロードなどを行うことができます。

16.8.1 証明書

*サイト間VPN > 証明書管理 > 証明書*を参照してください。

16.8.2 認証局 (CA)

*サイト間VPN > 証明書管理 > 認証局*を参照してください。

16.8.3 証明書失効リスト(CRL)

*サイト間VPN > 証明書管理 > 証明書失効リスト(CRL)*を参照してください。

16.8.4 詳細

*サイト間VPN > 証明書管理 > 詳細*を参照してください。

17 ログとレポート

この章では、Sophos UTMのログおよびレポート機能について説明します。

Sophos UTMは、各種システムおよびネットワーク保護イベントを継続的に記録することにより、豊富なログ機能を提供します。詳細な監査証跡により、過去と現在のさまざまなネットワークアクティビティに関する分析が実現し、潜在的なセキュリティ上の脅威を特定したり、発生している問題のトラブルシューティングを行うことができます。

Sophos UTMのレポート機能は、現在のログデータを収集し、それをグラフ形式で表示することで、管理対象デバイスのリアルタイム情報を提供します。

WebAdminのログパーティションステータスページは、ディスクの残容量、フィルアップレート(使用量増加速度)についての情報や、過去4週間のログパーティションの使用状況を示すヒ*ストグラムなど*、*Sophos UTMユニットのログパーティションのステータスを示します*。フィルアップレートは、測定地点と開始地点の差分を経過時間で割って計算するため、当初は値がやや不正確になりますが、システムの稼働時間が長くなればなるほど精度が増します。

この章には次のトピックが含まれます。

- ログファイルの閲覧
- ハードウェア
- ネットワーク使用状況
- ネットワークプロテクション
- Webプロテクション
- Eメールプロテクション
- リモートアクセス
- Webサーバプロテクション
- エグゼクティブレポート
- ログ設定
- レポート設定

レポートグラフ

Sophos UTMレポートデータを折れ線グラフや円グラフで表示します。対話的な性質上、これらのグラフでは情報にきめ細かくアクセスすることが可能となっています。

折れ線グラフ

折れ線グラフへの対話的操作が簡単です。マウスのカーソルをグラフ上に置くと、大きなドット(点)が表示され、グラフのその部分の詳細な情報が表示されます。このドットは、グラフの線に沿って移動します。マウスのカーソルを移動すると、ドットもそれに従って移動します。グラフに何本かの線がある場合、ドットはマウスカーソルの移動に従って線の間を移動します。さらに、ドットの色は、それが表示している情報がどの線に関連するかによって変わるため、線が互いに近接している場合に役立ちます。
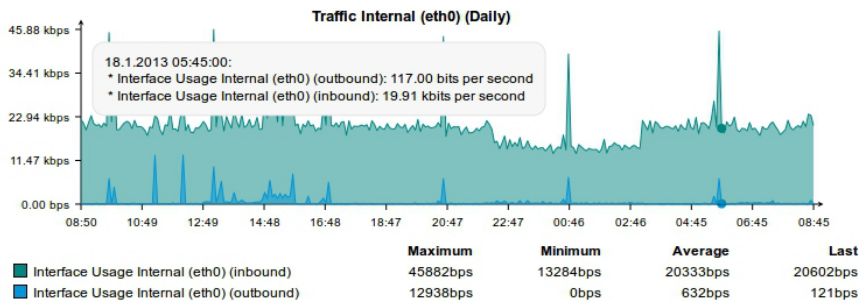
図 **31** レポート:折れ線グラフの例

円グラフ

円グラフも、折れ線グラフと同様に、インタラクティブ操作を行うことができます。マウスのカーソルを円グラフの一部に置きます。すると、その部分は円グラフの他の部分から即座に切り離され、その部分の詳細な情報がツールヒントに表示されます。
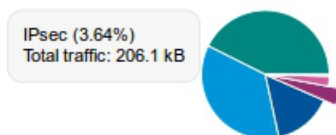
図 32 レポーティング:円グラフの例

17.1 ログファイルの閲覧

ログとレポート > *ログファイルの閲覧*メニューで、各種ログファイルを表示および検索できます。

17.1.1 今日のログファイル

ログとレポート > *ログファイルの閲覧* > *今日のログファイル*タブで、現在のすべてのログに容易にアクセスできます。

このタブでは、すべてのログファイルに適用できるさまざまな作業を実行できます。次の作業を実行できます。

- *ライブログ*:ポップアップウインドウが開き、リアルタイムでログファイルを表示できます。新しいアクティビティが発生すると、リアルタイムでログファイルに新しい行が追加されます。*自動スクロール*を選択すると、ポップアップウインドウが自動的スクロールダウンして、常に最新のログが表示されます。さらに、ポップアップウインドウにはフィルタテキストボックスも含まれており、これによって新しいログの表示ををフィルタに一致するレコードだけに制限できます。
- *表示*:ポップアップウィンドウが開き、ログファイルが現在の状態で表示されます。
- *クリア*:ログファイルのコンテンツを削除します。

テーブル下部のドロップダウンリストを使用して、選択したログファイルを`zip`ファイル形式でダウンロードしたり、それらのコンテンツを同時に削除したりできます。

17.1.2 アーカイブログファイル

ログとレポート > *ログファイルの閲覧* > *アーカイブログファイル*タブで、ログファイルアーカイブを管理することができます。すべてのログファイルはデイリーベースでアーカイブされます。アーカイブしたログファイルにアクセスするには、ログが書き込まれているSophos UTMのサブシステムと年月を選択します。

選択に一致したすべての利用できるログファイルが年代順に表示されます。アーカイブしたログファイルは、閲覧したり、zipファイル形式でダウンロードできます。

テーブル下部のドロップダウンリストを使用して、選択したログファイルをzipファイル形式でダウンロードしたり同時に削除したりすることができます。

17.1.3 ログファイルの検索

ログとレポート > *ログファイルの閲覧* > *ログファイルの検索*タブで、さまざまな期間のローカルログファイルを検索できます。最初に、検索するログファイルを選択し、次に検索する語句を入力して、検索期間を選択します。*期間を選択*リストから*カスタム期間*を選択した場合は、開始日と終了日を指定できます。*検索開始*ボタンをクリックすると、ポップアップウインドウにクエリ結果が表示されます。ブラウザによっては、WebAdmin用にポップアップウインドウを許可する必要があります。

*検索するログファイルの選択*リストから*Webフィルタリング*または*エンドポイントプロテクション*を選択すると、さらに3つのフィルタカテゴリが得られます。特定の*ユーザ*、*URL*、*ソースIP*および*アクション*を検索できます。

- **ユーザ**：ログの中で完全なユーザ名を検索できます。
- **URL**：URLと一致するサブ文字列を検索できます。
- **ソースIP**：アクティビティが開始されたソースIPです。
- **アクション**：あらゆる種類の可能なアクションを含んでいるドロップダウンリスト。

注 – *検索用語*の下で*チェックボックス*を選択すると、オプションで、ページ要求への結果に制限されますが、結果をレポートフォーマットで表示できます。また、*Webフィルタリング*や*エンドポイントプロテクション*で、同時に同じ検索を行うことができます。

17.2 ドウェア

ログとレポート > *ハードウェア*メニューには、さまざまな期間におけるハードウェアコンポーネントの使用状況に関する概要的な統計が表示されます。

17.2.1 デイリー

ハードウェア > *デイリー*タブは、次のハードウェアコンポーネントに関する過去24時間の統計概観を示します。

- CPUの使用状況
- メモリ/スワップ使用率
- パーティション使用率

CPUの使用状況:ヒストグラムに、現在のプロセッサ使用状況(%)が表示されます。

*メモリ/スワップ*の使用状況:メモリとスワップの使用状況(%)。スワップの使用状況は、システム構成によって大きく異なります。侵入防御やプロキシサーバなどのサービスをアクティブにすると、メモリの使用率が高くなります。システムのメモリが不足すると、スワップスペースが使用されるようになり、システム全体のパフォーマンスが低下します。スワップスペースの使用はできるだけ低く抑える必要があります。このためには、システムで利用できるメモリの合計容量を増やします。

*パーティション*使用状況:選択されたパーティションの使用状況(%)。すべてのチャートには3つのグラフが表示され、それぞれが1つのハードディスクドライブパーティションを示します。

- ルート: Sophos UTMルートパーティションとは、のルートディレクトリがあるパーティションです。このパーティションには、更新パッケージとバックアップも保存されます。
- ログ:ログパーティションとは、ログファイルとレポーティングデータが保存されるパーティションです。このパーティションの容量が不足している場合、*ログとレポート* > *ログ設定* > *ローカルログ*で設定を調整してください。
- ストレージ:ストレージパーティションとは、プロキシサービスがデータを保存するパーティションであり、Webフィルタ用の画像、SMTP プロキシ用のメッセージ、隔離メールなどがここに保存されます。さらに、データベース、一時データ、設定ファイルも保存されます。

17.2.2 ウィークリー

ハードウェア > *ウィークリー*タブは、選択されたハードウェアコンポーネントに関する過去7日間の概要的な統計を示します。ヒストグラムについては、*デイリー*のセクションを参照してください。

17.2.3 マンスリー

ハードウェア > *マンスリー*タブは、選択されたハードウェアコンポーネントに関する過去4週間の概要的な統計を示します。ヒストグラムについては、*デイリー*のセクションを参照してください。

17.2.4 年次

ハードウェア > *年次*タブは、選択されたハードウェアコンポーネントに関する過去12か月間の概要的な統計を示します。ヒストグラムについては、*デイリー*のセクションを参照してください。

17.3 ネットワーク使用状況

*ログとレポート> ネットワーク使用状況*メニューのタブには、さまざまな期間内にSophos UTMの各インタフェースを通過したトラフィックに関する概要的な統計が表示されます。各チャートのデータは、次の単位を使用して示されます。

- u（マイクロ、10^{-6}）
- m（ミリ、10^{-3}）
- k（キロ、10^{3}）
- M（メガ、10^{6}）
- G（ギガ、10^{9}）

10^{-18}～10^{8}の範囲内でスケーリング可能です。

17.3.1 デイリー

*ネットワーク使用状況 > デイリー*タブには、設定されている各インタフェースを通過するトラフィックに関する過去24時間の概要的な統計が表示されます。

各ヒストグラムには、次の2つのグラフが表示されます。

- 受信：該当インタフェースでの平均受信トラフィック（bps単位）。
- 送信：該当インタフェースでの平均送信トラフィック（bps単位）。

*同時接続*チャートは、同時接続の合計を示します。

17.3.2 ウィークリー

*ネットワーク使用状況 > ウィークリー*タブには、設定されている各インタフェースを通過するトラフィックに関する過去7日間の概要的な統計が表示されます。ヒストグラムについては、*デイリー*のセクションを参照してください。

17.3.3 マンスリー

*ネットワーク使用状況 > マンスリー*タブには、設定されている各インタフェースを通過するトラフィックに関する過去4週間の概要的な統計が表示されます。ヒストグラムについては、*デイリー*のセク

ションを参照してください。

17.3.4 年次

*ネットワーク使用状況 > 年次*タブには、設定されている各インタフェースを通過するトラフィックに関する過去12か月の概要的な統計が表示されます。ヒストグラムについては、*デイリー*のセクションを参照してください。

17.3.5 帯域使用状況

*ネットワーク使用状況 > 帯域使用状況*タブには、デバイスから転送されたネットワークトラフィック、デバイスに転送されたネットワークトラフィック、デバイスを経由して転送されたネットワークトラフィックについての包括的なデータが表示されます。

最初のドロップダウンリストから、表示するデータのタイプを選択します(例: *上位クライアント*や*上位サービス*、*クライアント別*など)。必要なエントリを選択し、追加でボックスが表示される場合は、該当するすフィルタの条件を指定します。または、下部にあるドロップダウンリストを使用して、時刻によってエントリをフィルタリングできます。必ず*更新*をクリックして、フィルタを適用します。

*クライアント別*および*サーバ別*ビューでは、IP/ネットワークやネットワーク範囲(例、`192.168.1.0/24`、`10/8`など)を手動で指定することができます。*サービス別*ビューでは、プロトコルとサービスをコンマで区切って入力することができます(*TCP*、*SMTP*、*UDP*、*6000*など)。プロトコルを指定しないと、TCPが使用されます(*HTTP*も有効です)。

*上位クライアント*および*上位サーバ*ビューで、結果の表でIPまたはホスト名をクリックすると、*クライアント別上位サービス*または*サーバ別上位サービス*ビューのフィルタとして自動的に使用されます。*上位サービス*、*上位アプリケーション*、*上位アプリケーションカテゴリ*ビューで、結果の表のサービス、アプリケーション、アプリケーションカテゴリをクリックすると、*サービス別上位クライアント*、*アプリケーション別上位クライアント*、*カテゴリ別上位クライアント*ビューのフィルタとして自動的に使用されます。

上位アプリケーション/*上位アプリケーションカテゴリ*: アプリケーションコントロールがオフの場合、ネットワークトラフィックは「未分類」と表示されます。アプリケーションコントロールが有効な場合、ネットワークトラフィックはタイプで表示されます(例 :「WebAdmin」、「NTP」、「facebook」)。アプリケーションコントロールに関する詳細は、*Webプロテクション > アプリケーションコントロール*の章を参照してください。

トラフィックのラベル *IN* と *OUT* は、視点に応じて異なります。プロキシモードで実行している場合、クライアントは(透過モードであっても)UTMでポート `8080` に接続するため、このクライアントか

ら送信されたデータ（要求）は内部インタフェースにおいて*受信*トラフィックとなり、クライアント宛てに送信されたデータ（応答）は*送信*トラフィックとなります。

デフォルトでは、1ページあたり20件表示されます。それを超える数のエントリがある場合は、「次へ」/「戻る」アイコンを使用して前後のページに移動できます。*行数*ドロップダウンリストで、1ページに表示するエントリの数を変更できます。

表の列見出しをクリックすると、すべてのデータを並べ替えることができます。たとえば、すべてのホストを受信トラフィック別にソートする場合、表の見出しで*IN*をクリックします。これにより、受信トラフィックが最も多く発生しているホストが先頭に表示されます。トラフィックのデータ量はキビバイト（KiB）およびメビバイト（MiB）単位で表示されます。いずれも、コンピュータの記憶容量を示す2の累乗単位です（例：1キビバイト = 2^{10}バイト = 1024バイト）。

タブ右上隅の対応するアイコンをクリックすると、データをPDFあるいはExcel形式でダウンロードできます。レポートは、現在選択されているビュー（表示）から生成されます。さらに、「円グラフ」アイコンが表示されている場合、それをクリックすると、表の上に円グラフが表示されます。

17.4 ネットワークプロテクション

*ログとレポート > ネットワークプロテクション*メニューのタブには、Sophos UTMによって検出された関連ネットワークプロテクションイベントについての概要的な統計が表示されます。

17.4.1 デイリー

*ネットワークプロテクション > デイリー*タブは、次のイベントに関する過去24時間の統計概観を示します。

- ファイアウォール違反
- 侵入防止の統計

ファイアウォール違反：ドロップまたは拒否されたすべてのデータパケットは、ファイアウォール違反としてカウントされます。ファイアウォール違反の回数は、5分間の枠内で計算されます。

IPS統計：すべてのチャートに、次の2つのグラフが表示されます。

- *アラートイベント*：侵入アラートをトリガしたデータパケットの数。
- *ドロップイベント*：侵入防御システムによってドロップされたデータパケットの数。

17.4.2 ウィークリー

*ネットワークプロテクション > ウィークリー*タブには、過去7日間以内に発生したファイアウォール違反および侵入防御イベントに関する概要的な統計が表示されます。ヒストグラムについては、*デイリー*のセクションを参照してください。

17.4.3 マンスリー

*ネットワークプロテクション > マンスリー*タブには、過去4週間以内に発生したファイアウォール違反および侵入防御イベントに関する概要的な統計が表示されます。ヒストグラムについては、*デイリー*のセクションを参照してください。

17.4.4 年次

*ネットワークプロテクション > 年次*タブには、過去12か月以内に発生したファイアウォール違反および侵入防御イベントに関する概要的な統計が表示されます。ヒストグラムについては、*デイリー*のセクションを参照してください。

17.4.5 ファイアウォール

*ネットワークプロテクション > ファイアウォール*タブには、ファイアウォールアクティビティに関する包括的なデータが、送信元IP、送信元ホスト、受信パケット数、サービス数に従って分類されて表示されます。

注 – TTL（生存時間）が1以下のパケットは、ログされることなくドロップされます。

最初のドロップダウンリストから、表示するデータのタイプを選択します（例: *上位送信元ホスト*や*上位サービス*、*宛先別*など）。必要なエントリを選択し、追加でボックスが表示される場合は、該当するすフィルタの条件を指定します。または、下部にあるドロップダウンリストを使用して、時刻によってエントリをフィルタリングできます。必ず*更新*をクリックして、フィルタを適用します。

*送信元別*および*宛先別*ビューでは、IP/ネットワークやネットワーク範囲（例、`192.168.1.0/24`、`10/8`など）を手動で指定することができます。*サービス別*ビューでは、プロトコルとサービスをコンマで区切って入力することができます（例、*TCP*、*SMTP*、*UDP*、*6000*など）。

*上位送信元ホスト*および*上位宛先ホスト*ビューで、結果の表でIPまたはホスト名をクリックすると、*送信元別上位サービス*または*宛先別上位サービス*ビューのフィルタとして自動的に使用され

ます。*上位サービス*ビューで、結果の表でサービスをクリックすると*サービス別上位送信元ホスト*ビューのフィルタとして自動的に使用されます。

デフォルトでは、1ページあたり20件表示されます。それを超える数のエントリがある場合は、「次へ」/「戻る」アイコンを使用して前後のページに移動できます。*行数*ドロップダウンリストで、1ページに表示するエントリの数を変更できます。

表の列見出しをクリックすると、すべてのデータを並べ替えることができます。

タブ右上隅の対応するアイコンをクリックすると、データをPDFあるいはExcel形式でダウンロードできます。レポートは、現在選択されているビュー(表示)から生成されます。さらに、「円グラフ」アイコンが表示されている場合、それをクリックすると、表の上に円グラフが表示されます。

17.4.6 高度な脅威防御

*ネットワークプロテクション > 高度な脅威防御*タブには、ネットワークでの脅威の詳細に関する包括的なデータが表示されます。

最初のドロップダウンリストから、表示するデータのタイプを選択します(例: *最新の感染*または*ホスト別最新の感染*。必要なエントリを選択し、追加でボックスが表示される場合は、該当するすフィルタの条件を指定します。または、下部にあるドロップダウンリストを使用して、時刻によってエントリをフィルタリングできます。必ず*更新*をクリックして、フィルタを適用します。

*最新のマルウェアによる感染*および*マルウェア別最新の感染*ビューでは、特定の脅威を手動でフィルタできます。*ホスト別最新の感染*ビューでは、特定のホストを手動でフィルタできます。

デフォルトでは、1ページあたり20件表示されます。それを超える数のエントリがある場合は、「次へ」/「戻る」アイコンを使用して前後のページに移動できます。*行数*ドロップダウンリストで、1ページに表示するエントリの数を変更できます。

表の列見出しをクリックすると、すべてのデータを並べ替えることができます。

タブ右上隅の対応するアイコンをクリックすると、データをPDFあるいはExcel形式でダウンロードできます。レポートは、現在選択されているビュー(表示)から生成されます。さらに、「円グラフ」アイコンが表示されている場合、それをクリックすると、表の上に円グラフが表示されます。

17.4.7 IPS

*ネットワークプロテクション > IPS*タブには、ネットワークでの侵入防御アクティビティに関する包括的なデータが表示されます。

最初のドロップダウンリストから、表示するデータのタイプを選択します(例: *上位送信元ホスト*や*上位宛先*、*送信元別*など)。必要なエントリを選択し、追加でボックスが表示される場合は、該当するすフィルタの条件を指定します。または、下部にあるドロップダウンリストを使用して、時刻によってエントリをフィルタリングできます。必ず*更新*をクリックして、フィルタを適用します。

*送信元別*および*宛先別*ビューでは、IP/ネットワークやネットワーク範囲(例、192.168.1.0/24、10/8など)を手動で指定することができます。*上位送信元ホスト*または*上位宛先ホスト*ビューで、結果の表でIPをクリックすると、*送信元別上位宛先*または*宛先別上位送信元*ビューのフィルタとして自動的に使用されます。

デフォルトでは、1ページあたり20件表示されます。それを超える数のエントリがある場合は、「次へ」/「戻る」アイコンを使用して前後のページに移動できます。*行数*ドロップダウンリストで、1ページに表示するエントリの数を変更できます。

表の列見出しをクリックすると、すべてのデータを並べ替えることができます。

タブ右上隅の対応するアイコンをクリックすると、データをPDFあるいはExcel形式でダウンロードできます。レポートは、現在選択されているビュー(表示)から生成されます。さらに、「円グラフ」アイコンが表示されている場合、それをクリックすると、表の上に円グラフが表示されます。

17.5 Webプロテクション

*ログとレポート > Webプロテクション*メニューのタブには、最もアクティブなWebユーザと最もよく表示されているWebサイトに関する概要的な統計が表示されます。

17.5.1 Web使用状況レポート

*ログとレポート > Webプロテクション > Web使用状況レポート*ページは、ネットワークトラフィックやユーザのWeb使用状況を確認するのに有用です。

Webサーフィンデータ統計

収集されるWebサーフィンデータはセッションベースです。UTMは、ユーザ毎のセッション(このユーザがどれくらいサーフィンしたか?)、ユーザおよびドメイン毎のセッション(このユーザが、このドメインでどれくらいサーフィンしたか?)、ドメインが上位レベルドメインにプラス1の重要レベルであるのはどこであるかなどを識別します。近似値を得るために、すべてのデータが以下のように収集されます。各Web要求は、トラフィック量および要求間隔を考慮に入れてログされます。5分間アクティビティがなく、セッションに対する要求が記録されないと、そのセッションは終了したものとみなされます。5分間アクティビティがない場合でもユーザがまだWebページを表示している可能性を考

えて、*経過時間*の値には常に1分余計に追加されます。レポーティングデータは15分ごとに更新されます。

したがって、たとえば10分間で、ユーザが2つのドメインの間で切り替えると、これはこのユーザに対しては合計10分の結果になりますが、このユーザによるドメインのサーフィンは20分になります。ただし、ユーザが異なるタブやブラウザを使って同じドメインをサーフィンした場合は、結果には影響しません。

クライアントが無効なURLを要求した場合、Webフィルタはその要求をログしますが、その要求に応えることはできません。これらのリンクは(エラー)ドメインとして計算されます。これらはレポーティングやWebフィルタのエラーではなく、ほとんどの場合、ページ作成者がWebコンテンツに無効または不正なリンクを配置したために発生します。

ページ構成

ヘッダバー

まず、次の要素から構成されているヘッダバーがあります。

- ホーム:このアイコンを使用して、クリックやフィルタをすべてクリアして最初の状態に戻すことができます。
- 前へ/次へ:これらのアイコンを使用して、変更や設定の履歴を前へ(または後ろへ)移動することができます。一般的なWebブラウザと同様に機能します。
- 利用可能なレポート:このドロップダウンリストには、保存されたレポート(もしあれば)を含む、利用可能なすべてのレポートタイプが含まれます。これはデフォルトで*サイト*に設定されています。*Web使用状況レポート*ページの結果テーブルは、このレポートタイプ設定に直接依存しています。

  > **注 –** フィルタを使用してレポートを次々にクリックすると、*利用可能なレポート*設定が自動的に変化するのを確認できます。これは常に、最新のレポート基準が反映されます。

  標準:レポートタイプは3種類あります。詳細は以下を参照してください。

  保存済み **Web** レポート: ここでは、過去に作成した、保存された Web レポートを選択できます。

- 削除:保存されたWebレポートを削除するには、このアイコンをクリックします。標準レポートは削除できません。

- 保存 : 現在のビューを保存して、後日このビューに簡単にアクセスできるようにするには、このアイコンをクリックします。これは*利用可能なレポート*ドロップダウンリストに保存されます。

フィルタバー

次に、次の要素から構成されているフィルタバーがあります。

- *プラス* + : このアイコンをクリックして、追加のフィルタを作成します。詳細は以下を参照してください。
- 件数 : ドロップダウンリストを使用して、テーブルに表示される結果を減らすことができます。結果を、上位10件、50件、100件の結果に制限することができます。
- 時間 : ドロップダウンリストを使用して、テーブルに表示される結果を、特定の時間枠内の結果に絞り込むか広げることができます。*カスタム*タイムフレームを選択すると、独自の時間枠を指定できます。
- 部門 : ドロップダウンリストを使用して、テーブルに表示される結果を、指定した部門に絞り込むことができます。部門は*部門*ページで作成できます。

フィルタバーの右側にある対応するアイコンをクリックすると、データをPDFあるいはExcel形式でダウンロードできます。レポートは、現在選択されているビュー(表示)から生成されます。さらに、円グラフのアイコンをクリックすると、表の上に円グラフが表示されます。送信アイコンをクリックすると、ダイアログウィンドウが開き、データを送信する前に、このレポートを受信する必要がある複数の受信者、件名やメッセージを入力することができます。また、保存されたレポートを定期的に受信することもできます。詳しくは*スケジュールされたレポート*を参照してください。

結果テーブル

表示内容は、選択されたレポートタイプおよび定義されたフィルタにより異なります。

> 注 – 匿名化を有効にすると、ユーザは名前やIPアドレスで表示される代わりに、数値で列挙されます。

レポートタイプに応じて、テーブルには異なる情報が表示されます。

#: 発生したトラフィックに関する順位。

トラフィック: 発生したトラフィックのサイズ

%: トラフィック全体に対する割合。

期間 : ユーザレポートタイプ : ユーザが滞在した時間。サイトレポートタイプ : ユーザがWebサイトに滞在した時間(すべてのユーザの合計)。

ページ：要求されたページ数（つまり、コード200およびcontent-type text/htmlで応答されたすべての要求）。

要求：カテゴリ、サイト、ドメイン、またはURL別のWeb要求数。

ユーザ：ブロックをバイパスしたユーザの名前。匿名化を有効にすると、*user_#*と表示されます。

使用されている割当て時間：使用された割当て時間の量です。

サイト：ブロックがバイパスされたサイト。

カテゴリ：あるURLが属するすべてのカテゴリが表示されます。カテゴリが複数存在する場合、カテゴリをクリックすると小さいダイアログフィールドが開き、いずれかのカテゴリを選択できます。このカテゴリに基づいてフィルタが作成されます。

アクション：Webサイトがクライアントに提供されたかどうか（*通過*）、アプリケーション制御ルールによって*ブロック*されたかどうか、ユーザがブロックバイパス機能を使用してブロックされたページにアクセスしたかどうか（*無視*）を表示します。

理由：Webサイト要求がブロックまたは無視された理由を表示します。例：ユーザが`msi`ファイルのダウンロードを試行し、ファイル転送を禁止するアプリケーションコントロールルールがあった場合、セルに理由が*msi*と表示されます。無視されたページの場合、ユーザが入力した理由が表示されます。

情報：利用可能な場合、このセルにはWebサイト要求がブロックされた理由を示す追加情報が表示されます（例：ファイルダウンロードが拡張子に基づいてブロックされた場合、セルには「拡張子（*extension*）」と表示されます）。

フィルタの定義

フィルタは、結果テーブルに表示される情報をドリルダウンするために使用されます。2とおりの定義方法があります。フィルタバーの「+」アイコンをクリックするか、テーブルをクリックします。

「+」アイコンを使用する場合：フィルタバーで緑の「+」アイコンをクリックすると、フィールドが2つある小さいフィルタバーが表示されます。1番目のフィールドのドロップダウンリストを使用すると、レポートタイプを選択できます（*カテゴリ*など）。2番目のフィールドを使用すると、選択したレポートタイプの値を選択するか入力することができます（例：*カテゴリ*を選んだ場合、*成人向けトピック*など）。*保存*をクリックしてフィルタを保存し、結果テーブルに適用します。

テーブルを使用する場合：テーブルをクリックし、クリックしたアイテムに複数のレポートタイプがある場合は、レポート方向が開きます。表示されたいずれかのオプションをフィルタ用に選択する必要があります。レポート方向ウィンドウを閉じると、関連フィルタが作成され、フィルタバーに表示されます。結果テーブルに、新たにフィルタされた結果が表示されます。

例：*Web使用状況レポート*のデフォルトレポートは*サイト*です。結果テーブルで、任意の行をクリックします（例：「amazon.com」）。*レポート方向*ウィンドウが開き、3つのオプションが提示されます。サ

イトの *ドメイン*に関する情報、サイトを訪問した*ユーザー*に関する情報、サイトが属する*カテゴリ*に関する情報のいずれかを参照することができます。複数のユーザが「amazon.com」を訪問したことがわかりました。さらに詳細を確認するために、*ユーザ*ボックスをクリックします。ウィンドウが閉じます。ヘッダバーではレポートタイプが*ユーザ*に変わり、フィルタバーでは*ユーザ*の結果テーブルが選択したサイト(「amazon.com」)によってフィルタされたことを確認できます。したがって、テーブルにはこのサイトを訪問したすべてのユーザと、これらのセッションに関する追加情報が表示されます。

> 注 – 一部のテーブルセルには独自のフィルタがあるため(上の*結果テーブル*セクションでアスタリスク(*)の付いたアイテム)、クリックしたテーブル行によって結果が異なる場合があります。

17.5.2 検索エンジンレポート

*ログとレポート > Webプロテクション > 検索エンジンレポート*ページには、ユーザが使用している検索エンジンやユーザが行った検索に関する情報が表示されます。一見するとこのページは非常に難解ですが、使用してみて結果を調べることから始めてみましょう。

ページ構成

ヘッダバー

まず、次の要素から構成されているヘッダバーがあります。

- ホーム:このアイコンを使用して、クリックやフィルタをすべてクリアして最初の状態に戻すことができます。
- 前へ/次へ:これらのアイコンを使用して、変更や設定の履歴を前へ(または後ろへ)移動することができます。一般的なWebブラウザと同様に機能します。
- 利用可能なレポート:このドロップダウンリストには、保存されたレポート(もしあれば)を含む、利用可能なすべてのレポートタイプが含まれます。これはデフォルトで*検索*に設定されています。*検索エンジンレポート*ページの結果テーブルは、このレポートタイプ設定に直接依存しています。

  > 注 – フィルタを使用してレポートを次々にクリックすると、*利用可能なレポート*設定が自動的に変化するのを確認できます。これは常に、最新のレポート基準が反映されます。

  標準:レポートタイプは3種類あります。詳細は以下を参照してください。

保存された検索エンジンレポート: ここでは、過去に作成した、保存された検索エンジンレポートを選択できます。

- 削除 : 保存された検索エンジンレポートを削除するには、このアイコンをクリックします。標準レポートは削除できません。
- 保存 : 現在のビューを保存して、後日このビューに簡単にアクセスできるようにするには、このアイコンをクリックします。これは*利用可能なレポート*ドロップダウンリストに保存されます。

フィルタバー

次に、次の要素から構成されているフィルタバーがあります。

- *プラス* **+** : このアイコンをクリックして、追加のフィルタを作成します。詳細は以下を参照してください。
- 件数 : ドロップダウンリストを使用して、テーブルに表示される結果を減らすことができます。結果を、上位10件、50件、100件の結果に制限することができます。
- 時間 : ドロップダウンリストを使用して、テーブルに表示される結果を、特定の時間枠内の結果に絞り込むか広げることができます。*カスタム*タイムフレームを選択すると、独自の時間枠を指定できます。
- 部門 : ドロップダウンリストを使用して、テーブルに表示される結果を、指定した部門に絞り込むことができます。部門は*部門*ページで作成できます。

フィルタバーの右側にある対応するアイコンをクリックすると、データをPDFあるいはExcel形式でダウンロードできます。レポートは、現在選択されているビュー(表示)から生成されます。さらに、円グラフのアイコンをクリックすると、表の上に円グラフが表示されます。送信アイコンをクリックすると、ダイアログウィンドウが開き、データを送信する前に、このレポートを受信する必要がある複数の受信者、件名やメッセージを入力することができます。また、保存されたレポートを定期的に受信することもできます。詳しくは*スケジュールされたレポート*を参照してください。

結果テーブル

最後に、結果テーブルがあります。ここに表示される結果は、第一に、選択したレポートタイプに依存し(*利用可能なレポート*リストに常に反映)、第二に、定義したフィルタに依存します。次のレポートタイプを使用できます。

- 検索 : ユーザが使用した検索文字列を表示します。
- 検索エンジン: ユーザが使用した検索エンジンを表示します。
- ユーザの検索 : 検索を行ったユーザを表示します。

注 – 匿名化を有効にすると、ユーザは名前やIPアドレスで表示される代わりに、数値で列挙されます。

それぞれのレポートタイプに対して、テーブルには以下の情報が表示されます。

#: 頻度に関する順位。

要求: 検索文字列、検索エンジン、ユーザ別の要求回数。

%: 検索全体に対する割合。

フィルタの定義

フィルタは、結果テーブルに表示される情報をドリルダウンするために使用されます。2とおりの定義方法があります。フィルタバーの「+」アイコンをクリックするか、テーブルをクリックします。

「+」アイコンを使用する場合: フィルタバーで緑の「+」アイコンをクリックすると、フィールドが2つある小さいフィルタバーが表示されます。1番目のフィールドのドロップダウンリストを使用すると、レポートタイプを選択できます(*検索エンジン*など)。2番目のフィールドを使用すると、選択したレポートタイプの値を選択するか入力することができます(例:*検索エンジン*を選んだ場合、*Google (google.com)*など)。*保存*をクリックしてフィルタを保存し、結果テーブルに適用します。検索用語は大文字と小文字が区別されず、ワイルドカードをサポート: ゼロまたはそれ以上の文字を一致させるには'*'を、1文字を一致させるには'?'を使用します。
テーブルを使用する場合: テーブルをクリックし、クリックしたアイテムに複数のレポートタイプがある場合は、*レポート方向*が開きます。表示されたいずれかのオプションをフィルタ用に選択する必要があります。*レポート方向*ウィンドウを閉じると、関連フィルタが作成され、フィルタバーに表示されます。結果テーブルに、新たにフィルタされた結果が表示されます。
例: *検索エンジンレポート*のデフォルトレポートは*検索*です。結果テーブルで、任意の行をクリックします(例:「天気」)。*レポート方向*ウィンドウが開き、2つのオプションが提示されます。検索に対して使用された検索エンジンに関する情報を表示するか(*検索エンジン*)、この文字列を検索したユーザーに関する情報を表示します(*ユーザー検索*)。複数のユーザが「天気」について検索したことがわかりました。さらに詳細を確認するために、*ユーザ検索*ボックスをクリックします。ウィンドウが閉じます。ヘッダバーでレポートタイプが*ユーザ検索*に変わり、フィルタバーで*ユーザ検索*の結果テーブルが選択した検索文字列(「天気」)によってフィルタされたことを確認できます。したがって、テーブルには「天気」について検索したすべてのユーザと、これらの検索に関する追加情報が表示されます。

17.5.3 部門

*ログとレポート > Webプロテクション > 部門*ページでは、ユーザまたはホストおよびネットワークを仮想部門にグループ化することができます。次に、これらの部門を使用してWeb使用状況レポートや検索エンジンレポートをフィルタすることができます。

部門を作成するには、次の手順に従います。

1. ***部門*タブで、*新規部門*をクリックします。**
   *部門の追加*ダイアログボックスが開きます。

2. **名前を入力します。**
   *名前*フィールドに、部門を説明する名前を入力します。

3. **ユーザまたはホスト/ネットワークを追加します。**
   部門の定義には、ユーザとホスト/ネットワークのいずれかしか含めることができず、両方を同時に含めることはできません。

   - ユーザ:この部門に加えるユーザを1人以上ボックスに追加します。
   - ホスト/ネットワーク:この部門に加えるホストまたはネットワークを1つ以上ボックスに追加します。

   コメント(オプション):説明などの情報を追加します。

4. ***保存*をクリックします。**
   新しい部門が*部門*リストに表示されます。

部門を編集、削除、または複製するには、対応するボタンをクリックします。

部門の使用について詳しくは、*Web使用状況レポート*と*検索エンジンレポート*のセクションを参照してください。

17.5.4 スケジュールレポート

*ログとレポート > Webプロテクション > スケジュールレポート*ページでは、定期的にEメールで送信したい保存済みレポートを定義することができます。スケジュールレポートを作成するためには、あらかじめ保存済みのレポートが少なくとも1つ必要です(レポートの保存については、*Web使用状況レポート*または*検索エンジンレポート*のセクションを参照)。

スケジュールされたレポートを作成するには、次の手順に従います。

1. *スケジュールされたレポート*タブで、*スケジュールされたレポートの追加*をクリックします。
   *スケジュールレポートの追加*ダイアログボックスが開きます。

2. 次の設定を行います。
   名前:スケジュールされたレポートを説明する名前を入力してください。

   間隔:ドロップダウンリストから、レポートを送信する間隔を選択します。

   レポート: 保存されたすべてのレポートがここに表示されます。選択した間隔で送信する各レポートの前にあるチェックボックスにチェックを入れてください。

   受信者:選択したレポートを受信する受信者をボックスに追加します。インポートボタンを使用して受信者のリストを追加することができます。

   コメント(オプション):説明などの情報を追加します。

3. *保存*をクリックします。

   新しいスケジュールされたレポートが*スケジュールされたレポート*リストに表示されます。

スケジュールされたレポートを編集、削除、または複製するには、対応するボタンをクリックします。スケジュールレポート自体を削除せずにレポートの送信を無効化するには、レポートのトグルスイッチを使用します。

17.5.5 アプリケーション コントロール

*ログとレポート > Webプロテクション > アプリケーション制御*ページには、様々な期間における最もアクティブな送信元、最も訪問が頻繁な宛先、最も人気の高いアプリケーションについての総合的な統計が表示されます。

最初のドロップダウンリストで、表示するデータのタイプを選択します。例、*上位ソース*または*上位アプリケーション*。必要なエントリを選択し、追加でボックスが表示される場合は、該当するすフィルタの条件を指定します。または、下部にあるドロップダウンリストを使用して、時刻によってエントリをフィルタリングできます。必ず*更新*をクリックして、フィルタを適用します。

*送信元別*および*宛先別*ビューでは、IP/ネットワークやネットワーク範囲(例、`192.168.1.0/24`、`10/8`など)を手動で指定することができます。*サービス別*ビューでは、プロトコルとサービスをコンマで区切って入力することができます(例、*TCP*、*SMTP*、*UDP*、*6000*など)。

*上位ソース*ビューで、結果の表でIPまたはホスト名をクリックすると*ソース別上位アプリケーション*ビューのフィルタとして自動的に使用されます。*上位アプリケーション*および*上位アプリケーションカテゴリ*ビューで、結果の表でアプリケーションまたはアプリケーションカテゴリをクリックすると、*アプ*

*リケーション元別上位送信元*または*アプリケーションカテゴリ別上位送信元*ビューのフィルタとして自動的に使用されます。

デフォルトでは、1ページあたり20件表示されます。それを超える数のエントリがある場合は、「次へ」/「戻る」アイコンを使用して前後のページに移動できます。*行数*ドロップダウンリストで、1ページに表示するエントリの数を変更できます。

表の列見出しをクリックすると、すべてのデータを並べ替えることができます。

タブ右上隅の対応するアイコンをクリックすると、データをPDFあるいはExcel形式でダウンロードできます。レポートは、現在選択されているビュー（表示）から生成されます。さらに、「円グラフ」アイコンが表示されている場合、それをクリックすると、表の上に円グラフが表示されます。

最もアクティブな送信元はすぐには表に表示されず、セッションタイムアウトの発生後に表示されます。たとえば、特定クライアント（ユーザ名またはIPアドレス）が5分間Webサーフィンを停止したとします。この場合、UTMはこのサーフィンセッションを「デッド」と判断し、最もアクティブな送信元リストに表示する前にデータベースに送ります。

17.5.6 非匿名化

*Webプロテクション > 非匿名化*タブは、匿名化が有効になっている場合のみアクセス可能です（*ログとレポート > レポーティング設定 > 匿名化*を参照）。

ここでは、Webプロテクションレポートに関する特定ユーザの匿名化をやめることができます。次の手順で実行します。

1. **両方のパスワードを入力します。**
   匿名化を有効にするために指定した1番目と2番目のパスワードを入力します。
2. **非匿名化にするユーザを追加します。**
   *ユーザの非匿名化*ボックスに、非匿名にするユーザのユーザ名を追加します。
3. ***適用*をクリックします。**
   設定が保存されます。

17.6 Eメールプロテクション

*ログとレポート > Eメールプロテクション*メニューのタブには、メールフロー、メール使用状況、およびEメールプロテクションについての概要的な統計が表示されます。

17.6.1 使用状況グラフ

*Eメールプロテクション > 使用状況グラフ*タブには、さまざまな時間枠内にUTMを通過したメールフローの概要的な統計が表示されます。

- デイリー
- ウィークリー
- マンスリー
- 年次

17.6.2 メール使用状況

*Eメールプロテクション > メール使用状況*タブには、さまざまな時間帯で最もアクティブに使用されたEメールアドレスやアドレスドメインに関する包括的な統計が表示されます。

最初のドロップダウンリストで、表示するデータのタイプを選択します。例、*上位送信者*または*上位ドメイン*。必要なエントリを選択し、追加でボックスが表示される場合は、該当するすフィルタの条件を指定します。または、下部にあるドロップダウンリストを使用して、時刻によってエントリをフィルタリングできます。必ず*更新*をクリックして、フィルタを適用します。

*ドメイン別*および*アドレス別*ビューでは、ドメインまたはアドレスを手動で指定することができます。ドメインの指定では、パーセント記号(%)をワイルドカードとして使用できます。キーワード末尾にパーセント記号を付けた場合は、完全一致または部分一致を検索するようにSophos UTMに指示することになります。フィルタフィールドでは大文字と小文字が区別されます。

*上位アドレス*および*上位ドメイン*ビューで、結果の表でアドレスまたはドメインをクリックすると、*ドメイン別上位アドレス*または*アドレス別上位ピア*ビューのフィルタとして自動的に使用されます。

デフォルトでは、1ページあたり20件表示されます。それを超える数のエントリがある場合は、「次へ」/「戻る」アイコンを使用して前後のページに移動できます。*行数*ドロップダウンリストで、1ページに表示するエントリの数を変更できます。

表の列見出しをクリックすると、すべてのデータを並べ替えることができます。

タブ右上隅の対応するアイコンをクリックすると、データをPDFあるいはExcel形式でダウンロードできます。レポートは、現在選択されているビュー(表示)から生成されます。さらに、「円グラフ」アイコンが表示されている場合、それをクリックすると、表の上に円グラフが表示されます。

17.6.3 ブロックメール

Eメールプロテクション > *ブロッメール*タブには、ウイルス対策およびアンチスパムによってブロックされたすべてのメール要求に関する包括的な統計が表示されます。

最初のドロップダウンリストで、表示するデータのタイプを選択します。例、*上位ブロックされたスパムの理由*または*上位ブロックされたマルウェア*。必要なエントリを選択し、追加でボックスが表示される場合は、該当するすフィルタの条件を指定します。または、下部にあるドロップダウンリストを使用して、時刻によってエントリをフィルタリングできます。必ず*更新*をクリックして、フィルタを適用します。

*上位ブロックされたドメイン*ビューで、結果の表のドメインをクリックすると*ドメイン別上位ブロックされたアドレス*ビューのフィルタとして自動的に使用されます。*ドメイン別*ビューでは、ドメインを手動で指定することができます。パーセント記号(%)をワイルドカードとして使用できます。キーワード末尾にパーセント記号を付けた場合は、完全一致または部分一致を検索するようにSophos UTMに指示することになります。フィルタフィールドでは大文字と小文字が区別されます。

デフォルトでは、1ページあたり20件表示されます。それを超える数のエントリがある場合は、「次へ」/「戻る」アイコンを使用して前後のページに移動できます。*行数*ドロップダウンリストで、1ページに表示するエントリの数を変更できます。

表の列見出しをクリックすると、すべてのデータを並べ替えることができます。

タブ右上隅の対応するアイコンをクリックすると、データをPDFあるいはExcel形式でダウンロードできます。レポートは、現在選択されているビュー(表示)から生成されます。さらに、「円グラフ」アイコンが表示されている場合、それをクリックすると、表の上に円グラフが表示されます。

17.6.4 非匿名化

Eメールプロテクション > *非匿名化*タブは、匿名化が有効になっている場合のみアクセス可能です(*ログとレポート* > *レポーティング設定* > *匿名化*を参照)。

ここでは、Eメールプロテクションレポートで特定のEメールアドレスやドメインの匿名化を中止することができます。次の手順で実行します。

1. **両方のパスワードを入力します。**
   匿名化を有効にするために指定した1番目と2番目のパスワードを入力します。

2. **次の設定を行います。**
   アドレスの非匿名化:非匿名化するEメールアドレスを追加します。

ドメインの非匿名化：非匿名化するドメインを追加します。

3. *適用*をクリックします。
設定が保存されます。

指定したメールアドレスとドメインはレポートに表示されるようになります。

17.7 ワイヤレスプロテクション

*ログとレポート > ワイヤレスプロテクション*メニューのタブには、Sophos UTMによって検出された関連ワイヤレスプロテクションイベントについての概要的な統計が表示されます。

17.7.1 デイリー

*ワイヤレスプロテクション > デイリー*タブには、ワイヤレスネットワークやアクセスポイントに関する過去24時間の概要的な統計が表示されます。

SSID別レポーティング

それぞれのワイヤレスネットワークのチャートがあります。各チャートには、次の2つのグラフが表示されます。

- 接続されているクライアント：ワイヤレスネットワークに接続されているクライアントの数。
- 失敗した接続試行：ワイヤレスネットワークで失敗した接続試行の回数。

AP別レポーティング

それぞれのアクセスポイントについて、テーブルは最大および平均の接続ユーザ、アップタイム（過去24時間の間にアクセスポイントがアップであった累積時間）、ならびに再接続の回数を示します。

17.7.2 ウィークリー

*ワイヤレスプロテクション > ウィークリー*タブには、ワイヤレスネットワークやアクセスポイントに関する過去7日間の概要的な統計が表示されます。ヒストグラムについては、*デイリー*のセクションを参照してください。

17.7.3 マンスリー

*ワイヤレスプロテクション > マンスリー*タブには、ワイヤレスネットワークやアクセスポイントに関する過去4週間の概要的な統計が表示されます。ヒストグラムについては、*デイリー*のセクションを参照してください。

17.7.4 年次

*ワイヤレスプロテクション > 年次*タブには、ワイヤレスネットワークやアクセスポイントに関する過去12か月間の概要的な統計が表示されます。ヒストグラムについては、*デイリー*のセクションを参照してください。

17.8 リモートアクセス

*ログとレポート > リモートアクセス*メニューのタブは、リモートアクセスアクティビティおよびセッション情報に関する全体的な統計を提供します。

17.8.1 アクティビティ

*リモートアクセス > アクティビティ*タブは、さまざまな期間についてIPsec、SSL VPN、PPTP、およびL2TPのUTMのリモートアクセスアクティビティに関する統計概要を提供します。

- デイリー
- ウィークリー
- マンスリー
- 年次

期間を選択:ドロップダウンリストを使用して、レポート期間を選択します。ページは自動的にリロード(再読み込み)されます。

17.8.2 セッション

*リモートアクセス > セッション*タブは、さまざまな時間範囲について、完了したセッション、失敗したログイン、および現在のユーザに関する包括的な統計を提供します。

注 – *アップ*および*ダウン*の列は、リモートアクセス接続のアカウンティングデータを示しています。システムの負荷が増えるので、アカウンティングはデフォルトで無効です。*リモートアクセスアカウンティング*セクションの *レポーティング設定* > *設定*タブで有効にすることができます。

最初のドロップダウンリストで、表示したいセッションのタイプを選択できます。*現在のユーザ*、*完了したセッション*、*失敗したログイン*。*更新*ボタンをクリックし、フィルタを適用します。

2番目のドロップダウンリストを使用すると、結果をフィルタできます。選択したセッションのタイプに応じて、異なるフィルタが使用できます。例、*サービス別*、*送信元IPアドレス別*。一部のフィルタでは、フィルタ引数を選択または入力する必要があります。

3番目のドロップダウンリストを使用すると、結果を時間別にフィルタできます。必ず*更新*をクリックして、フィルタを適用します。

デフォルトでは、1ページあたり20件表示されます。それを超える数のエントリがある場合は、「次へ」/「戻る」アイコンを使用して前後のページに移動できます。*行数*ドロップダウンリストで、1ページに表示するエントリの数を変更できます。

表の列見出しをクリックすると、すべてのデータを並べ替えることができます。

タブ右上隅の対応するアイコンをクリックすると、データをPDFあるいはExcel形式でダウンロードできます。レポートは、現在選択されているビュー(表示)から生成されます。さらに、「円グラフ」アイコンが表示されている場合、それをクリックすると、表の上に円グラフが表示されます。

17.9 Webサーバプロテクション

ログとレポート > *Webサーバプロテクション*メニューのタブは、Webサーバの要求、警告、アラートに関する概要的な統計を表示します。

17.9.1 使用状況グラフ

Webサーバプロテクション > *使用状況グラフ*タブは、さまざまな時間枠内にUTMで発生したWebサーバの要求、警告、アラートに関する概要的な統計を表示します。

- デイリー
- ウィークリー
- マンスリー
- 年次

17.9.2 詳細

*Web サーバプロテクション > 詳細*タブには、さまざまな時間枠内で最もアクティブだったクライアント、仮想ホスト、バックエンド、応答コード、および様々な攻撃に関する包括的な統計が表示されます。

最初のドロップダウンリストで、表示するデータのタイプを選択します。例、*上位クライアント*または*仮想ホスト毎上位攻撃者*。必要なエントリを選択し、追加でボックスが表示される場合は、該当するすフィルタの条件を指定します。または、下部にあるドロップダウンリストを使用して、時刻によってエントリをフィルタリングできます。必ず*更新*をクリックして、フィルタを適用します。

*クライアント別*および*攻撃者別*ビューでは、IP/ネットワークやネットワーク範囲(例、`192.168.1.0/24`、`10/8`など)を手動で指定することができます。*仮想ホスト別*ビューでは、ドメインを手動で指定することができます。パーセント記号(`%`)をワイルドカードとして使用できます。キーワード末尾にパーセント記号を付けた場合は、完全一致または部分一致を検索するようにSophos UTMに指示することになります。フィルタフィールドでは大文字と小文字が区別されます。

*上位クライアント*または*上位攻撃者*ビューで、結果の表でIPをクリックすると、*クライアント別上位応答コード*または*攻撃者別上位ルール*ビューのフィルタとして自動的に使用されます。

デフォルトでは、1ページあたり20件表示されます。それを超える数のエントリがある場合は、「次へ」/「戻る」アイコンを使用して前後のページに移動できます。*行数*ドロップダウンリストで、1ページに表示するエントリの数を変更できます。

表の列見出しをクリックすると、すべてのデータを並べ替えることができます。

タブ右上隅の対応するアイコンをクリックすると、データをPDFあるいはExcel形式でダウンロードできます。レポートは、現在選択されているビュー(表示)から生成されます。さらに、「円グラフ」アイコンが表示されている場合、それをクリックすると、表の上に円グラフが表示されます。

17.10 エグゼクティブレポート

*ログとレポート > エグゼクティブレポート*メニューでは、各サービスのネットワーク使用状況を表示するために重要なレポーティングデータをグラフィカルな形式にまとめることができます。

17.10.1 レポートを見る

*ログとレポート > エグゼクティブレポート > レポートを見る*タブでは、*レポーティング*メニューのタブとページにある個々のレポートに基づいて、完全なエグゼクティブレポートを作成することができま

す。エグゼクティブレポートを表示するウィンドウを開くには、*レポートの作成*ボタンをクリックします。

17.10.2 アーカイブエグゼクティブレポート

エグゼクティブレポート > *アーカイブエグゼクティブレポート*タブには、アーカイブされたすべてのエグゼクティブレポートの概要が表示されます。*設定*タブでアーカイブが選択されているエグゼクティブレポートのみがアーカイブされます。

17.10.3 設定

エグゼクティブレポート > *設定*タブでは、エグゼクティブレポートの設定を行うことができます。

デイリーエグゼクティブレポート

デイリーエグゼクティブレポート: 有効にすると、デイリーエグゼクティブレポートが作成されます。

PDF *レポートをアーカイブ*: 有効にすると、デイリーエグゼクティブレポートがPDF 形式でアーカイブされます。アーカイブされたエグゼクティブレポートには、*アーカイブされたエグゼクティブレポート*タブでアクセスできます。

HTMLの*代わりに***PDF** *としてレポートを送信*: 有効にすると、メールで送信するデイリーエグゼクティブレポートがPDF ファイルとして添付されます。選択を解除すると、HTML 形式で送信されます。

メールアドレス: エグゼクティブレポートを受信する必要がある受信者のメールアドレスを入力します。

ウィークリーエグゼクティブレポート

大部分の設定については、*デイリーエグゼクティブレポート*のセクションを参照してください。

このレポートでは、エグゼクティブレポートがデータの収集を開始する曜日も選択できます。

マンスリーエグゼクティブレポート

大部分の設定については、*デイリーエグゼクティブレポート*のセクションを参照してください。

17.11 ログ設定

ログとレポート > *ログ設定*メニューで、ローカルおよびリモートログの基本的な設定を構成できます。

17.11.1 ローカルログ

ログとレポート > *ログ設定* > *ローカルログ*タブで、ローカルログの設定を行うことができます。デフォルトではローカルログは有効になっています。

ただし、ローカルログが無効になっている場合は、以下の手順で有効にできます。

1. ***ローカルログ*タブでローカルログを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチが緑色に変わり、このタブ内のエリアが編集可能になります。

2. **ログファイルを削除する時間枠を選択します。**
   ドロップダウンリストから、ログファイルに自動的に適用するアクションを選択します。デフォルトでは、*ログファイルを削除しない*が選択されています。

3. ***適用*をクリックします。**
   設定が保存されます。

   トグルスイッチが緑色に変わります。

しきい値

ここでローカルログのしきい値を定義できます。しきい値は、この値に達した場合に実行される特定のアクションに結び付けられます。次の作業を実行できます。

- なし：何も起こりません。
- 通知の送信：しきい値に達したことを管理者に伝える通知を送信します。
- 古いログから削除：残りの量が設定したしきい値より下になるまで、あるいはログファイルのアーカイブが空になるまで、一番古いログファイルが削除されます。さらに、そのアクションの通知が管理者に送信されます。
- システムのシャットダウン：システムがシャットダウンします。そのイベントの通知が管理者に送信されます。システムをシャットダウンする場合は、管理者はローカルログの設定を変更し、ログファイルの削除を設定するか、あるいはログファイルを手動で移動/削除する必要があります。システムシャットダウンの理由が持続する場合は、次回のログ消去プロセスの実行時（毎日午前 12:00 つまり真夜中に実施）にシステムは再び自らをシャットダウンします。

設定を保存するには*適用*をクリックします。

17.11.2 リモートSyslogサーバ

ログとレポート > *ログ設定* > *リモートSyslog サーバー*タブで、リモートログの設定を行うことができます。この機能により、UTMから他のホストにログメッセージを転送できます。これは、ホストを使用していくつかのUTMからログ情報を収集するネットワークに特に役立ちます たホストでは、Syslog プロトコル互換のログデーモンを実行する必要があります。

リモート syslog サーバーを設定するには、以下の手順に従います。

1. ***リモートSyslog サーバー*タブでリモート syslog を有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、*リモートSyslog 設定*エリアが編集可能になります。

2. ***Syslog サーバー*ボックスの「+」アイコンをクリックしてサーバーを作成します。**
   *Syslog サーバーの追加*ダイアログボックスが開きます。

3. **次の設定を行います。**
   名前：リモートsyslogサーバを説明する名前を入力します。

   サーバ: UTMからログを受信する必要があるホストを追加または選択します。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

   警告 – UTM自体のインタフェースをリモート syslog ホストとして使用しないでください。これを行うと、ログループになります。

   ポート: 接続に使用するサービス定義を追加または選択します。定義を追加する方法は、*定義とユーザ* > *ネットワーク定義* > *ネットワーク定義*ページで説明しています。

4. ***適用*をクリックします。**
   設定が保存されます。

   トグルスイッチが緑色に変わります。

リモートsyslogバッファ

このエリアで、リモート syslog のバッファサイズを変更できます。バッファサイズはバッファに保持されるログの行数です。デフォルトは1000です。設定を保存するには*適用*をクリックします。

Syslog送信ログ選択

このエリアはリモート syslog が有効なときのみ編集できます。syslog サーバーに送信するログのチェックボックスにチェックを入れてください。*すべてを選択*オプションを選択すると、一度にすべて

のログを選択することができます。設定を保存するには*適用*をクリックします。

17.11.3 リモートログファイルアーカイブ

*ログとレポート> ログ設定 > リモートログファイルアーカイブ*タブで、ログファイルのリモートアーカイブを設定することができます。リモートログファイルのアーカイブを有効にすると、前日のログファイルは1つのファイルに集約・圧縮され、リモートログファイルのストレージに転送されます。ドロップダウンリストで転送方法を選択できます。

リモートログファイルのアーカイブを設定するには、以下の手順に従います。

1. ***リモートログファイルアーカイブ*機能を有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、*リモートログファイルアーカイブ*エリアが編集可能になります。

2. **ログファイルのアーカイブ方式を選択します。**
   ドロップダウンリストで、希望のアーカイブ方式を選択します。選択した方式に応じて、各アーカイブ方式に関連する設定オプションが下に表示されます。以下のアーカイブ方式から選択できます。

   - **FTPサーバ:** *ファイル転送プロトコル*(FTP)方式では、以下のパラメータを設定する必要があります。

     - ホスト: FTPサーバのホストの定義。
     - サービス: サーバがリスンするTCPポート。
     - ユーザ名 : FTPサーバアカウントのユーザ名。
     - パスワード: FTPサーバアカウントのパスワード。
     - パス: ログファイルが保存されているリモート(相対)パス。

   - **SMB CIFS シェア:** SMB方式では、以下のパラメータの設定が必要です。

     - ホスト: SMBサーバのホストの定義。
     - ユーザ名 : SMBアカウントのユーザ名。
     - パスワード: SMBアカウントのパスワード。

> セキュリティ注 – パスワードは設定ファイルにプレーンテキストで保存されます。したがって、このログに固有のユーザー/パスワードの組み合わせを作成することをお勧めします。

- 共有: SMB共有名。ログファイルの転送先のパスまたはネットワーク共有情報を入力します(例: `/logs/logfile_archive`)。
- ワークグループ/ドメイン: ログファイルのアーカイブを入れるワークグループまたはドメインを入力します。

- **Secure Copy SSH**サーバ : SCP方式を使用するには、公開SSH DSA鍵を、お使いのSCPサーバの承認済み鍵に追加する必要があります。Linuxシステムでは、SSH DSA鍵をカット&ペーストして、設定されたユーザアカウントの`~/.ssh/authorized_keys`ファイルに追加できます。インストール時にSophos UTMによって新しいSSHDSA鍵が作成されます。セキュリティ上の理由から、このSSH DSA鍵はバックアップには含まれません。したがって、新規またはバックアップのインストール後に、新しいSSH DSA鍵をリモートサーバーに保存して、ログファイルのアーカイブをSCPサーバーに安全にコピーできるようにする必要があります。

  > 注 – WindowsでのSSHキーの作成およびアップロードについての詳細は、Opengearヘルプデスクでご確認ください。

  SCP方式には以下の設定が必要です。

  - ホスト: SCPサーバのホストの定義。
  - ユーザ名: SCPサーバアカウントのユーザ名。
  - パス: ログファイルの保存先の(完全な)リモートパス。
  - 公開**DSA**鍵: リモートストレージホスト上で、提供された公開DSA鍵を承認済み鍵のリストに追加します。

- メール送信: ログファイルのアーカイブをメールで送信できるように、有効なメールアドレスを入力します。

3. *適用*をクリックします。
   設定が保存されます。

トグルスイッチが緑色に変わります。

転送が失敗すると、アーカイブはUTMに残ります。それぞれのログ削除プロセス時に、UTMは残りのすべてのアーカイブを配信しようと試みます。

17.12 レポート設定

*ログとレポート > レポート設定*メニューで、レポーティングの特定機能の有効化/無効化やデータ保持時間/量の設定といったレポーティング機能の設定を行うことができます。さらに、プライバシ保護を強化するためにデータを匿名にすることができます。

17.12.1 設定

*設定*タブで、*レポートア*クションおよびレポートデータが自動的に削除されるまでのシステムでの保持期間を定義できます。以下のレポートトピックを設定できます。

- アプリケーションコントロール
- 認証
- Eメールプロテクション
- ファイアウォール
- IPS
- ネットワーク使用状況
- リモートアクセス
- Webプロテクション
- Webサーバープロテクション

左側のチェックボックスを使用して、特定トピックに関するレポートを有効/無効にします。デフォルトでは、すべてのレポートトピックが有効になっています。

右側のドロップダウンリストを使用して、レポートデータの保持期間を設定します。

注 – 不要なレポートを無効にすることで、マシンの基本的な負荷を減らし、パフォーマンスのボトルネックを削減できます。レポートの保持期間はできるだけ短く設定してください。保存データの量が多いと基本的な負荷が高くなり、動的なレポートページの応答性を低下させます。

このタブの設定は、ログファイルアーカイブへは影響しません。

Webプロテクションレポート詳細レベル

このセクションでは、Webプロテクションレポートの詳細レベルを定義することができます。詳細レベルを高くすると、メモリの使用量とシステム負荷が目に見えて増加するため、必要でない限りは、詳細レベルを低くしてください。

以下の詳細レベルを設定できます。

- ドメインのみ:レポートには、URLのトップレベルドメインとセカンドレベルドメイン(例:`example.com`)が表示されます。サードレベルドメインは、強制すると表示されます(例:`example.co.uk`)。
- フルドメイン:レポートには、フルドメインが表示されます(例:`www.example.com`、`shop.example.com`
- **1**レベルの**URL**:レポートには、URLの最初の(仮想)ディレクトリが追加で表示されます(例:`www.example.com/en/`)。
- **2**レベルの**URL**:レポートには、URLの最初から2つの(仮想)ディレクトリが追加で表示されます(例:`www.example.com/en/products/`)。
- **3**レベルの**URL**:レポートには、URLの最初から3つの(仮想)ディレクトリが追加で表示されます(例:`www.example.com/en/products/new/`)。

エグゼクティブレポート設定

このエリアで、保持するエグゼクティブレポートの数をそれぞれ定義できます。

- デイリーレポート:最大60
- ウィークリーレポート:最大52
- マンスリーレポート:最大12

設定を保存するには*適用*をクリックします。

エグゼクティブレポートとそのオプションに関する詳細は、*ログとレポート* > *エグゼクティブレポート*を参照してください。

PDF用紙設定

PDFエグゼクティブレポートのデフォルトの用紙サイズはA4です。ドロップダウンリストを使用して、*レター*または*リーガル*を選択できます。設定を保存するには*適用*をクリックします。

リモートアクセスアカウンティング

ここで、リモートアクセス接続に対してアカウンティングを有効または無効にできます。有効にすると、リモートアクセス接続に関するデータが、*ログとレポート* > *リモートアクセス* > *セッション*タブの*ダウ*

*ン*および*アップ*の列に保存および表示されます。無効にすると、アカウンティングは停止します。有効にすると、システムへの負荷が増大することに注意してください。

CSV区切り文字設定

ここでは、CSV形式へのレポーティングデータのエクスポート時に使用するデリミタを定義できます。Windowsオペレーティングシステムでは、エクスポートするデータがExcelなどの表計算プログラムで正確に表示されるようにするために、デリミタがシステムの地域設定と一致する必要があります。

IPFIXアカウンティング

IPFIXを使用して、UTMのIPv4フローデータをプロバイダにエクスポートし、モニタリング、レポート、アカウンティング、料金請求などのために使用することができます。

IPFIX（Internet Protocol Flow Information Export）は、アカウンティング情報を普遍的な方法でエクスポートするためのメッセージベースのプロトコルです。アカウンティング情報は、*エクスポータ*により収集され、*コレクタ*に送信されます。IPv4フローの一般的なアカウント情報は、*送信元アドレス*、*宛先アドレス*、*送信元ポート*、*宛先ポート*、*バイト*、*パケット*、*およびネットワークトラフィック分類データ*で構成されます。

有効にすると、UTMがエクスポータとして機能します。IPFIXアカウンティングデータをエクスポートします。コレクタは通常プロバイダのサイトに配置され、ここで1つ以上のUTMのアカウンティングデータが集約されて分析されます。プロバイダでのシステムのセットアップ時にホスト名が提供され、1つのエクスポータ、つまりUTM毎に一意のOID（Observation Domain ID）を定義する必要があります。このデータを該当するフィールドに入力します。

データは、UDP ポート4739でエクスポートされます。1つのネットワーク接続が、エクスポート方向のために1つと応答のために1つの合計2つのIPFIXフローを使用します。

> セキュリティに関する注記 – IPFIXでは、アカウンティングデータが暗号化されずに転送されることに注意してください。したがって、データは必ずプライベートネットワークだけで送信することが推奨されます。

設定を保存するには*適用*をクリックします。

IPFIXプライベートエンタープライズ番号

UTMで使用されるテンプレートは、プライベートエンタープライズ番号（PEN）9789 _Astaro AG and 21373 _netfilter/iptables project_を参照しています。以下の要素を利用可能です。

名前	ID	タイプ	エンター プライズ	意味
マーク	4	uint32_t	Netfilter	Netfilterコネクショントラッキングマーク。
conntrack_id	6	uint32_t	Netfilter	NetfilterコネクショントラッキングID。
afcProtocol	1	uint16_t	Astaro	Astaro Flow Classifierにより検出されるプロトコル。このフィールドは、識別子がオフであっても常に表示されます。識別子がプロトコルを検出できなかった場合、「不明」を意味するプロトコルID 0がレポートされます。
afcProtocolName	2	文字列	Astaro	ゼロ終端32文字のASCII文字列として、Astaro Flow Classifierにより検出されるプロトコル名。
flowDirection	4	uint8_7	Astaro	フローの方向、内 1 、外 2 、または内でも外でもない 0 のいずれか。各フローは2回エクスポートされます。各方向につき1回です。

17.12.2 除外

レポート設定 > *除外*タブで、特定のドメインやアドレスをレポートから除外できます。これはエグゼクティブレポートに加え、*ログとレポート*ページと統計概要ページに影響を及ぼします。

注 – 今日の統計ページの情報は、10～15分毎に更新されるのみであるため、この影響が統計ページに直ちに表れるわけではありません。インポート機能によって複数の項目を一度に定義することも可能です。

レポーティング除外：web

このセクションには、すべてのWebプロテクションレポートから除外するドメインを定義できます。ドメイン名には、*ログとレポート* > *Web プロテクション* > *Web 使用状況レポート*タブの*ドメイン*レポートにリストされたものとまったく同じ名前を指定する必要があります。設定を保存するには*適用*をクリックします。

レポーティング除外：メール

これらの2つのセクションには、すべてのメールプロテクションレポートから除外するドメインとメールアドレスを定義できます。

特定のドメインのすべてのメールアドレスを除外するには、*ドメイン*ボックスを使用します。sophos.comのように、メールアドレスのドメイン部分のみを入力します。レポートから特定のメールアドレスを除外するには、*アドレス*ボックスを使用します。設定を保存するには*適用*をクリックします。

指定したドメイン名またはアドレスを含む送信者または受信者のメールが、すべてのメールプロテクションレポートから除外されます。

レポーティング除外：ネットワークプロテクション

このセクションには、すべてのネットワークプロテクションレポートから除外するIPv4およびIPv6アドレスを定義できます。設定を保存するには*適用*をクリックします。

レポーティング除外：ネットワークアカウンティング

このセクションには、すべてのネットワーク使用状況レポートから除外するIPv4およびIPv6アドレスを定義できます。設定を保存するには*適用*をクリックします。

17.12.3 匿名化

レポート設定 > *匿名化*タブでは、「4つの目の原則」に基づいてレポートデータを匿名にできます。これは、2人の人間がその手順を承認した場合のみ非匿名化できることを意味します。匿名にすると、ユーザデータのレポートを表示する際にそのデータの機密性が保たれるため、アクション（Webサーフィンなど）から特定の人間にトレースバックする（さかのぼる）ことができなくなります。

匿名にするには、以下の手順に従います。

1. ***匿名化*タブで匿名化を有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、*匿名化設定*エリアが編集可能になります。

2. **2つのセキュリティパスワードを入力します。**
   「4つの目の原則」は、異なる2人の人間が互いが秘匿しているパスワードを入力したときのみ有効です。

3. ***適用*をクリックします。**
   設定が保存されます。

   トグルスイッチが緑色に変わります。

匿名化を再度グローバルに無効にするには、その両方のパスワードが必要になります。

1. ***匿名化*タブで、トグルスイッチをクリックします。**
   トグルスイッチがアンバー色になり、*匿名化設定*エリアが編集可能になります。

2. **両方のパスワードを入力します。**
   匿名化を有効にするために指定した1番目と2番目のパスワードを入力します。

3. ***適用*をクリックします。**
   設定が保存されます。

   トグルスイッチが緑色に変わります。

必要に応じて、匿名化を1人のユーザに対して無効にできます。詳細は*ログとレポート > Webプロテクション*および*ログとレポート > Eメールプロテクション*を参照してください。

18 サポート

この章では、Sophos UTMで使用できるサポートツールについて説明します。

*サポート*メニューのページには、さまざまな Web リンク、お問い合わせ情報、役立つネットワークツールの出力など、お客様サポート関連の多数の機能が含まれています。これらを活用されることで、UTM のコマンドラインインタフェースを使用しないで、重要なネットワークプロパティを判断することができます。

この章には次のトピックが含まれます。

- ドキュメント
- 印刷可能形式設定情報
- サポート窓口
- ツール
- 詳細

さらに、*サポート*メニューのメインページには、以下の情報への Web リンクが含まれています。

- ナレッジベース(KB):Sophos NSGの公式Knowledgebaseには、Sophos UTMの設定に関するさまざまな情報が掲載されています。
- 既知の問題のリスト(KIL):解決できない既知の問題や対応策のある既知の問題のリストです。
- ハードウェア互換性リスト(HCL):Sophos UTMソフトウェアに対応するハードウェアのリストです。
- **Up2Date情報:** Sophos NSGUp2Dateブログには、製品の改善やファームウェアの更新についての情報が掲載されています。

18.1 ドキュメント

オンラインヘルプ

このセクションでは、オンラインヘルプの開き方や使用方法を説明します。

マニュアルのダウンロード

管理ガイドマニュアルのダウンロード ガイドの言語を選択し、*ダウンロード開始*をクリックします。PDF文書を開くためには、Adobe ReaderやXpdfといった専用のリーダーが必要です。

クロスリファレンス – UTMの以前のバージョンの管理ガイドやその他のドキュメントは、Sophos Knowledgebaseからダウンロードできます。

18.2 印刷可能形式設定情報

*サポート > 印刷可能形式設定情報*ページでは、現在のWebAdmin設定について詳細なレポートを作成できます。

注 – 印刷可能設定は新しいウィンドウで開きます。ブラウザによっては、WebAdmin用にポップアップウインドウを許可する必要があります。

印刷可能設定の構造は、WebAdminメニューの構造と同じであるため、対応するWebAdminの設定オプションを簡単に見つけることができます。

印刷可能設定ブラウザページは、概要ページ(*索引*)と複数のサブページから成ります。サブページへのリンクはブルーでハイライトされています。サブページには、関連トピックの詳細情報が表示されます。サブページの下部にある*索引に戻る*リンクをクリックして、いつでもサブページから索引に戻ることができます。

印刷可能設定には他に2つの表示オプションがあります。

- WebAdmin形式
- Confd形式

これらの表示オプションへのリンクは、索引ページの下部にあります。

18.3 サポート窓口

Sophosは、セキュリティソリューションのために総合的なカスタマーサポートサービスを提供しています。お客様の サポート/メンテナンスレベルに応じて、さまざまなレベルのアクセスサービスに加え、Sophos サービス部門や Sophos NSG 認定パートナーによるさまざまなレベルのサポートを提供しています。

Sophos UTMに関連するすべてのサポートケースは、MyUTM ユーザガイド経由で処理されます。サポートケースを開くには、*新しいウィンドウでサポートチケットをオープンする*をクリックして Web フォームを使用してください。詳しくは、MyUTM ユーザガイドを参照してください。

18.4 ツール

サポート> *ツール*メニューのタブには、有用なネットワークツールの出力が表示されます。これらを使用すると、UTMのコマンドラインインタフェースを使用しないで、重要なネットワークプロパティを判断することができます。ここでは、以下のツールの出力を見ることができます。

- Ping
- Traceroute
- DNSルックアップ

18.4.1 Pingチェック

*ping*プログラムは、IPネットワークを横断して特定ホストに到達できるかどうかをテストするためのコンピュータネットワークツールです。ping は、ICMP *エコー要求*パケットをターゲットホストに送信し、ICMP *エコー応答*による返信を待機することで機能します。ping は、間隔のタイミングと応答率を使用して、ホスト間の往復時間とパケット紛失率を評価します。

pingチェックを行うには、以下の手順に従います。

1. **pingホストを選択します。**
   pingするホストを選択します。*Pingホスト*ボックスで、ホスト定義のあるホストを選択できます。または、*ホスト名/IPアドレスを入力*を選択してカスタムホスト名またはIPアドレスを下のテキストボックスに入力することもできます。

2. **IPバージョンを選択します(IPv6をグローバルに有効にしている場合にのみ使用できます)。**
   *IPバージョン*ドロップダウンリストで、*IPv4*または*IPv6*を選択します。

3. **インタフェースを選択します。**
   pingを経由させるインタフェースを選択します。

4. ***適用*をクリックします。**
   pingチェックの出力が*Pingチェック結果*エリアに表示されます。

18.4.2 トレースルート

traceroute（トレースルート）プログラムは、IPネットワーク上でパケットが使用するルートの決定に使用されるコンピュータネットワークツールです。tracerouteは、パケットの伝送に関与したルータのIPアドレスを一覧表示します。一定の時間内にパケットのルートを判断できない場合は、IPアドレスの代わりにアスタリスク(*)で報告します。一定の回数だけ失敗すると、確認作業は終了します。確認の中断には多くの理由が考えられますが、ほとんどの場合は、ネットワークパスのファイアウォールが traceroute パケットをブロックすることが原因となります。

ルートを追跡するには、以下の手順に従います。

1. **トレースルートホストを指定します。**
   ルートをトレースしたいホストを選択します。*トレースルートホスト*ボックスで、ホスト定義があるホストを選択できます。または、*ホスト名/IPアドレスを入力*を選択してカスタムホスト名またはIPアドレスを下のテキストボックスに入力することもできます。
2. **IPバージョンを選択します（IPv6をグローバルに有効にしている場合にのみ使用できます）。**
   *IPバージョン*ドロップダウンリストで、*IPv4*または*IPv6*を選択します。
3. インタフェースを選択します。
   トレースルートに使用するインタフェースを選択します。
4. **ホップアドレスをホスト名解決せず、数字で表示** *オプション* 。
   パスで見つかった各ゲートウェイについて、ネームサーバでIPアドレスからDNSホスト名への名前解決を行わない場合は、このオプションを選択します。
5. ***適用*をクリックします。**
   tracerouteの出力が *トレースルートの結果*エリアに表示されます。

18.4.3 DNSルックアップ

*ホスト*プログラムは、DNSネームサーバに問い合わせを行うネットワークツールです。digプログラムはDNSルックアップを実行し、クエリしたネームサーバから返された応答を表示します。

DNSルックアップを行うには、以下の手順に従います。

1. **ホスト名/IPアドレスを指定します。**
   DNS情報を判定したいホストのホスト名またはIPアドレスを入力します。
2. ***詳細出力の有効化*を選択します** *オプション* 。
   このオプションを選択すると、より詳細な情報が出力されます。

3. ***適用*をクリックします。**
   digの出力が*DNSルックアップの結果*エリアに表示されます。

18.5 詳細

*サポート > 詳細*メニューには、UTMに関するより詳細な情報が表示され、高度な機能にアクセスできます。ここには、実行中のプロセスとローカルネットワーク接続の概要が表示され、ルーティングテーブルとインタフェーステーブルを確認することができます。さらに、デバッグやリカバリのためのサポートパッケージをダウンロードしたり、ログファイルに表示される内部使用の設定リファレンスに関する背景情報を確認することができます。

18.5.1 プロセスリスト

*ps*プログラムは、ヘッダ行に続き、コントロール端末を持つプロセスに関する情報を表示します。この情報は、コントロール端末毎にソートされ、次にプロセスID毎にソートされます。

18.5.2 LAN コネクション

プログラム*netstat*(*ネットワーク統計*の略語)とは、コンピュータに現在存在するアクティブなインターネット接続(受信と送信の両方)のリストを表示するネットワークツールです。

18.5.3 ルーティングテーブル

*ip*コマンドは、TCP/IPネットワークのコントロールとトラフィックコントロールのためのネットワークツールです。パラメータ`route show table all`付きで実行されるこのプログラムは、UTMのすべてのルーティングテーブルの内容を表示します。

18.5.4 インタフェーステーブル

このテーブルには、Sophos UTMのすべての設定済みインタフェース(ネットワークインタフェースカードと仮想インタフェースの両方)が表示されます。`addr`パラメータ付きで実行した*ip*プログラムが、インタフェースとそのプロパティを表示します。

18.5.5 コンフィグダンプ

デバッグやリカバリのために、Sophos UTMのインストールに関してできるだけ多くの情報を収集しておくと便利です。*サポート* > *詳細* > *コンフィグダンプ*タブでダウンロードできるサポートパッケージは、これに対応します。zipファイルには次のアイテムが含まれています。

- UTMの設定の全ダンプ（storage.abf）。これは真のバックアップファイルではないため、パスワードなどが含まれておらず、デバッグ目的のみで使用できます。
- システム内に存在するハードウェアに関する情報（hwinfo）。
- システムにインストールされたソフトウェアパッケージに関する情報（swinfo）。

18.5.6 REF_ をリゾルブ

デバッグのために、システム内部で使用されている設定リファレンスを解決することができます。ログ内でリファレンスを見つけた場合、リファレンス文字列をここに貼り付けてください（例：REF_DefaultSuperAdmin）。タブに、設定用Configurationデーモンのデータ構造の該当箇所が表示されます。

19 ログオフ

UTMからログアウトするには、*ログオフ*メニューエントリをクリックします。適切にログアウトしなかった場合や、Webブラウザを誤って閉じてしまった場合には、約30秒間再ログインできない可能性があります。

注 – セッション中に別のWebサイトにアクセスした場合にも、ログアウトしたことになります。この場合、ログインしなおす必要があります。

20 ユーザポータル

この章は、ユーザポータルの動作方法に関する情報や、どのサービスがエンドユーザに提供されるかを説明しています。

Sophos UTMのユーザポータルは、許可されたユーザにパーソナルなメールおよびリモートアクセスサービスを提供する特別なブラウザベースアプリケーションです。ユーザーポータルにアクセスするには、Sophos UTMの URL（`https://192.168.2.100`など）にブラウズします（HTTPS プロトコル）。

ログインページで、ユーザはヘッダバーの右側にあるドロップダウンリストから言語を選択できます。

管理者によってどのサービスや機能がWebAdminで有効化されているかに応じて、ユーザは以下のサービスにアクセスできます：

- メール隔離
- メールログ
- POP3アカウント
- 送信者ホワイトリスト
- 送信者ブラックリスト
- ホットスポット
- クライアント認証
- OTPトークン
- リモートアクセス
- HTML5 VPNポータル
- パスワードの変更
- HTTPSプロキシ

ワンタイムパスワード機能が有効であれば、一定の条件下でログインした場合に、複数のQRコードを示す長いページが表示されます。ログインページが表示されるのは、*ユーザ機能のOPTの自動作成*トークンが有効で、ユーザが自分独自のパスワードだけを使ってログインしており（ワンタイムパスワードを追加せず）、そのユーザについて未使用のOTPトークンが使用可能である場合だけです。このページには、モバイルデバイスを設定して、ワンタイムパスワードを生成するための指示が表示されます。モバイルデバイスを設定すると、今度はUTMパスワードを使用して、ワンタ

イムパスワードを続けて入力し、再度ログインすることができます。例 : 使用しているUTMパスワードが`1z58.xa`であり、ワンタイムパスワードが`123456`であるなら、単に`1z58.xa123456`と入力するだけでログインできます。

20.1 ユーザポータル : メール隔離

このタブで、エンドユーザは隔離場所に保持されているメッセージを表示したりリリースしたりすることができます。

> **注** – *メール隔離*タブは、WebAdminでPOP3またはSMTPが有効で、これらのサービスを使用するようにユーザが設定している場合に使用できます。ユーザがSMTP とPOP3の両方でメールを受信する場合は、メールが*POP3隔離*および*SMTP隔離*の2つのタブに編成されます。これらのタブの機能は同じです。

*メール隔離*タブには、ユーザ宛てに送信され、Sophos UTMによってブロックと隔離が行われたすべてのEメールの概要が表示されます。リストされる必要があるPOP3隔離メールについて、ユーザはPOP3資格情報を*POP3アカウント*タブで入力する必要があります。

隔離メールのソートとフィルタ

デフォルトではすべてのメールが表示されます。リストに 20件を超えるメールが含まれる場合、複数ページに分割され、「>」(次へ)ボタンと「<」(戻る)ボタンを使用して移動することができます。

表示オプションを変更するには、次の手順に従います。

Sort by ソート順 : デフォルトでは、受信時刻によりリストがソートされています。ここでは、別のソート基準を選択できます。

and show 表示 : チェックボックスで、ページ当たり20、50、100、250、500、1000、またはすべてのメッセージを表示できます。すべてのメッセージの表示には時間がかかる場合があります。

ページのいくつかの要素を使用してメールをフィルタすることができます。

- **#隔離** *メッセージ*: ページの上部にあるいくつかのチェックボックスを使用すると、隔離理由(マルウェア、スパム、表現との一致、ファイル拡張子、MIMEタイプ、スキャン不可能など)によってメールを表示したり、非表示にすることができます。
- *アドレスまたはアカウント*: 受信者のアドレス(SMTP)またはアカウント(POP3)に応じて、メッセージをフィルタすることができます。

- 送信者/受信者/件名サブストリング: ここでは、隔離されたメッセージ内で検索する送信者、受信者 (POP3のみ)、または件名を入力します。
- 受信日 : 特定の期間内に処理されたメッセージのみを表示するには、日付を入力するか、カレンダアイコンで日付を選択します。

隔離メールの管理

ユーザは、メッセージの前にあるドロップダウンリストを使用してメッセージにアクションを適用することができます。また、複数の選択したメッセージにアクションを適用することもできます それぞれのメッセージのの前にあるチェックボックスを使用するか、メッセージをクリックして選択します。次に、テーブルの下にあるドロップダウンリストを使用して、適用可能なアクションを1つ選択します。次の作業を実行できます。

- 表示 (個別のメッセージでのみ使用可能) : メールのコンテンツを示すウィンドウを開きます。
- ダウンロード: 選択したメッセージは、EML形式でダウンロードされます。
- 削除 : 選択されたメッセージを削除します。これを取り消すことはできません。
- 送信者のホワイトリスト化 (個別のメッセージでのみ使用可能) : メールを受信トレイに移動し、送信者をホワイトリストに追加します (*送信者ホワイトリスト*タブ)。この送信者から送られる後のメールが隔離されないようになります。悪質なコンテンツを含むメールは、ホワイトリストの送信者から送られている場合でも、常に隔離されます。
- リリース: 選択されたメッセージを隔離からリリースします。
- リリースし、誤検出として報告 : 選択したメッセージを隔離からリリースし、スパムスキャンエンジンに誤検出として報告します。

注 – ここで可能なアクションは、メールの隔離理由とWebAdmin設定に依存します。ユーザは、明示的に許可されているメッセージのみをリリースすることができます。隔離に保留されているメッセージをすべてリリースできるのは管理者だけです。

グローバルクリーンアップアクションの選択 : ここには、メッセージに対してグローバルに適用されるさまざまな削除オプションがあります。つまり、選択されていないメッセージや表示されていないメッセージにもオプションが適用されます。

20.2 ユーザポータル: メールログ

このタブで、エンドユーザがSMTPで送信されるメールトラフィックのログを表示することができます。

> 注 – *メールログ*タブは、ユーザのメールアドレスがSophos UTMのSMTPプロキシによりモニタリングされるドメインに属し、管理者によってユーザにこの機能のアクセス権が割り当てられている場合にのみ表示されます。SMTP とPOP3の両方が特定のユーザについて有効であれば、このタブは*SMTP ログ*と呼ばれます。

*メールログ*タブには、ユーザのメールアドレスのすべてのメールトラフィックに関するログエントリが示されます。未配信のメールのログエントリには、配信されなかった理由に関する情報が含まれます。ログエントリをダブルクリックすると、ウィンドウが開き、詳細なログ情報が表示されます。

デフォルトではすべてのメールが表示されます。リストに 20件を超えるメールが含まれる場合、複数ページに分割され、「>」(次へ)ボタンと「<」(戻る)ボタンを使用して移動することができます。

表示オプションを変更するには、次の手順に従います。

Sort by ソート順 : デフォルトでは、受信時刻によりリストがソートされています。ここでは、別のソート基準を選択できます。

and show 表示 : チェックボックスで、ページ当たり20、50、100、250、500、1000、またはすべてのメッセージを表示できます。すべてのメッセージの表示には時間がかかる場合があります。

ページのいくつかの要素を使用してメールをフィルタすることができます。

- **#**ファイルのログイベント: ページの上部にあるいくつかのチェックボックスを使用すると、そのステータスに応じてメールを表示したり、非表示にすることができます。
- アドレス: 送信者アドレスに応じてメールをフィルタできます。
- 送信者/件名 サブストリング: ここでは、隔離されたメッセージ内で検索する送信者、受信者、または件名を入力します。
- 受信日 : 特定の期間内に処理されたメッセージのみを表示するには、日付を入力するか、カレンダアイコンで日付を選択します。

20.3 ユーザポータル:POP3アカウント

このタブで、エンドユーザは隔離されたメールの表示とリリース、および隔離レポートの受信が可能かどうかを確認できます。

注 – *POP3アカウント*タブを使用できるのは、管理者がPOP3を有効にしていて、POP3サーバを追加している場合だけです。

このページで、使用するPOP3アカウントの資格情報を入力する必要があります。POP3アカウントの資格情報が与えられたスパムメールのみがユーザポータルに表示されます。POP3アカウントの資格情報が保存されているユーザは、各Eメールアドレスについて個々の隔離レポートを受け取ります。

20.4 ユーザポータル:送信者ホワイトリスト

このタブでは、エンドユーザがメール送信者をホワイトリスト化し、それらの送信者からのメッセージを常にスパムとしないことができます。ただし、ウイルスを伴うメールや、スキャン不能なメールは引き続き隔離されます。

注 – *送信者ホワイトリスト*タブは、ユーザのメールアドレスがSophos UTMによりモニタリングされるネットワークまたはドメインに属し、管理者によってユーザにこの機能のアクセス権が割り当てられている場合にのみ表示されます。

ホワイトリストに送信者を追加するには、「+」アイコンをクリックしてアドレスを入力し、チェックアイコンをクリックして保存します。有効なメールアドレスを入力するか(`jdoe@example.com`など)、アスタリスクをワイルドカードとして使用して特定ドメインのすべてのメールアドレスを指定できます(`*@example.com`など)。送信者ホワイトリストと送信者ブラックリストを組み合わせて使用することができます:たとえば、ドメイン全体(例、`*@hotmail.com`)はブラックリスト化しながら、このドメインに属している特定のメールアドレス(例、`mycolleague@hotmail.com`)をホワイトリスト化することができます。また、これを反対に機能させることもできます。正確なメールアドレスがホワイトリストとブラックリストの両方にあると、そのアドレスはブラックリスト化します。

20.5 ユーザポータル:送信者ブラックリスト

On this tab, end-users can blacklist email senders, so the messages from them are always regarded as spam and therefore will be quarantined.

注 – *送信者ブラックリスト*タブは、ユーザのメールアドレスがSophos UTMによりモニタリングされるネットワークまたはドメインに属し、管理者によってユーザにこの機能のアクセス権が割り当てられている場合にのみ表示されます。

ブラックリストは、システム内でSMTPとPOP3が使用されていれば、SMTPとPOP3の両方のメールに適用されます。ブラックリストに送信者を追加するには、「+」アイコンをクリックしてアドレスを入力し、チェックアイコンをクリックして保存します。有効なメールアドレスを入力するか(`jdoe@example.com`など)、アスタリスクをワイルドカードとして使用して特定ドメインのすべてのメールアドレスを指定できます(`*@example.com`など)。送信者ホワイトリストと送信者ブラックリストを組み合わせて使用することができます:たとえば、ドメイン全体(例、`*@hotmail.com`)はブラックリスト化しながら、このドメインに属している特定のメールアドレス(例、`mycolleague@hotmail.com`)をホワイトリスト化することができます。また、これを反対に機能させることもできます。正確なメールアドレスがホワイトリストとブラックリストの両方にあると、そのアドレスはブラックリスト化します。

20.6 ユーザポータル:ホットスポット

ホットスポット機能により、カフェ、ホテル、企業などではゲストに時間制限やトラフィック制限を課したインターネットアクセスを提供できます。

注 – ユーザポータルの*ホットスポット*タブは、管理者が*パスワード*か*バウチャー*タイプのホットスポットを作成し、ユーザを許可ユーザに追加している場合にのみ表示されます。

このタブでは、ワイヤレスネットワークのゲストにホットスポットアクセス情報を配信できます。可能な機能は、選択したホットスポットのタイプに応じて、一般的なパスワードを配信するか、バウチャーを生成して配信するかのいずれかになります。

ホットスポットタイプ: 当日有効パスワード

*パスワード*フィールドには、現在のパスワードが表示されます。パスワードは1日に1回自動的に変更されます。ただし、手動でパスワードを変更することもできます。パスワードを変更すると、古いパスワードが即時に無効になり、アクティブなセッションが終了します。

パスワードを変更するには、次の手順に従います。

1. **ユーザポータルで、*ホットスポット*タブを選択します。**
2. **アクセス情報を管理するホットスポットを選択します。**
   *ホットスポット*ドロップダウンリストから、パスワードを変更するホットスポットを選択します。
3. **新しいパスワードを定義する必要があります。**
   *パスワード*フィールドに新しいパスワードを入力するか、*生成*ボタンをクリックして自動的に新しいパスワードを作成します。
4. **新しいパスワードをメールで送信するには、*メール送信*チェックボックスにチェックを入れます。**
   管理者によって指定されているメール受信者にパスワードが送信されます。管理者がメールアドレスを指定していない場合は、チェックボックスは使用できません。
5. ***保存*をクリックする必要があります。**
   パスワードが即時に変更されます。

ホットスポットタイプ: バウチャー

それぞれ一意のコードを持つバウチャーを作成することができます。バウチャーは印刷してゲストに提供することができます。作成したバウチャーのリストにより、バウチャーの使用状況を把握および管理できます。

バウチャーを作成するには、次の手順に従います。

1. **ユーザポータルで、*ホットスポット*タブを選択します。**
2. **以下の設定を行う必要があります。**
   ホットスポット: バウチャーを作成したいホットスポットを選択する必要があります。

   バウチャー定義 : 使用可能なバウチャータイプは管理者によって定義されています。どの目的にどのタイプのバウチャーを使用するかは、社内で定義する必要があります。

   件数 : このタイプのバウチャーの作成数を入力する必要があります。

コメント: オプションで、コメントを入力することができます。このコメントはユーザのバウチャーリストに表示されます。

印刷: ユーザが直接バウチャーを印刷したい場合は、このオプションを選択する必要があります。

ページサイズ: 印刷するページサイズを選択する必要があります。

ページ当たりのバウチャー数: 1ページに印刷するバウチャーの数を選択します。UTMが、ページ当たりのバウチャー数を自動的に調整します。

QR *コードの追加*: バウチャーのテキストデータに加えて、印刷されるバウチャーにQRコードを追加することができます。QRコードとは、エンコードされたデータを含んでいる正方形の画像です。ホットスポットのログインページにアクセスするためにモバイルデバイスでスキャンすることができ、フィールドには必要なデータが入力されます。

3. *バウチャーの作成*ボタンをクリックする必要があります。
   バウチャーが生成されます。下のバウチャーリストの新しい行に、各バウチャーが即時に表示されます。印刷を指定した場合は、バウチャーが直接印刷されます。各バウチャーには、一意のコードがあります。

注 – バウチャーの内容、サイズ、レイアウトは管理者によって設定されます。

バウチャーリストでバウチャーを管理することができます。リストの並べ替えやフィルタ、コメントの入力または変更、選択したバウチャーの印刷、削除、エクスポートを行うことができます。

- リストを並べ替えるには、*ソート基準*ドロップダウンリストから目的のソート基準を選択する必要があります。右のドロップダウンリストを使用すると、1ページに表示するバウチャーの数を変更できます。
- リストをフィルタするには、*ステータス*、*コード*、*コメント*のいずれかのフィールドを使用する必要があります。必要な属性をそれぞれ選択するか、入力します。入力するにつれ、リストが直接フィルタされます。フィルタをリセットするには、ステータスエントリの *すべて*を選択し、*コード*や *コメント*テキストフィールドからすべてのテキストを削除する必要があります。
- コメントを入力するか変更する場合は、各バウチャーの *コメント*列にあるメモ帳アイコンをクリックする必要があります。編集フィールドが表示されます。テキストを入力するか編集してEnterキーを押すか、チェックマークをクリックして変更を保存できます。
- バウチャーを印刷するか削除するには、目的のバウチャーの前にあるチェックボックスにチェックを入れ、下部にある必要なボタンをクリックする必要があります。

> 注 – バウチャーは、一定の時間の経過後に自動的に削除することができます。この時間は管理者が設定できます。

- バウチャーをエクスポートするには、目的のバウチャーの前にあるチェックボックスにチェックを入れ、下部にある*CSVへのエクスポート*ボタンをクリックする必要があります。ウィンドウが表示され、CSVファイルを保存するか、CSVファイルを直接開くかを選択できます。選択したバウチャーが1つのCSVファイルに保存されます。ファイルを開く際には、列の区切り文字として正しい文字を選択するようにしてください。

20.7 ユーザポータル：クライアント認証

このタブで、エンドユーザはSophos Authentication Agent（SAA）のセットアップファイルをダウンロードできます。SAAはWebフィルタの認証モードとして使用できます。

> 注 – *クライアント認証*タブは、管理者によってクライアント認証が有効化されている場合にのみ使用できます。

20.8 ユーザポータル：OTP トークン

このタブでは、エンドユーザがQRコードやデータにアクセスして、モバイルデバイスにOTP構成をインストールすることができます。

Google認証システムでOTPトークンを設定する

1. モバイルデバイスに**Google**認証システムをインストールします。
2. **QR**コードをスキャンします。
3. **アプリを起動します。**
   30秒後に変化するワンタイムパスワードが表示されます。
4. **ワンタイムパスワードを使用する対象の機能を起動します。**
   ワンタイムパスワードを入力する必要があるサービス、たとえば、リモートアクセスの接続、Webアプリケーションファイアウォール、ユーザポータル自体などは管理者が設定しています。
5. **資格情報を入力します。**

ユーザ名とUTMパスワードを入力し、続けて現在のワンタイムパスワードを入力します。

6. *ログイン*ボタンをクリックします。
   これで、その機能にアクセスできるようになります。

他のソフトウェアの使用

1. モバイルデバイスにソフトウェアをインストールします。
2. アプリを起動します。
3. **QRコードのそばにあるデータを使用して、アプリを設定します。**
   これで、アプリがワンタイムパスワードを生成します。
4. **ワンタイムパスワードを使用する対象の機能を起動します。**
   ワンタイムパスワードを入力する必要があるサービス、たとえば、リモートアクセスの接続、Webアプリケーションファイアウォール、ユーザポータル自体などは管理者が設定しています。
5. **資格情報を入力します。**
   ユーザ名とUTMパスワードを入力し、続けて現在のワンタイムパスワードを入力します。
6. *ログイン*ボタンをクリックします。
   これで、その機能にアクセスできるようになります。

20.9 ユーザポータル：リモートアクセス

このタブでは、管理者が行ったWebAdmin設定に従って自動的に生成され、提供されるリモートアクセスクライアントのソフトウェアや設定ファイルをエンドユーザがダウンロードすることができます。

注 – *リモートアクセス*タブは、ユーザに対して最低1つのリモートアクセスモードが有効になっている場合のみ利用できます。

管理者がユーザに対して有効にしている接続タイプに対応するリモートアクセスデータのみが提供されます。たとえば、SSLVPNリモートアクセスのみが有効にされている場合、*SSL VPN*セクションのみが表示されます。

各接続タイプが別のセクションに表示されます。接続タイプによっては、各ソフトウェアをダウンロードするための情報やボタンがあります。該当する場合は、セクションの上部に*新しいウィンドウ*

*でインストール手順を開く*リンクが表示されます。これをクリックすると、詳細なインストール手順が開きます。

20.10 ユーザポータル : HTML5 VPNポータル

HTML5 VPNポータルを使用すると、外部ネットワークのユーザは、ブラウザのみをクライアントとして使用して、あらかじめ設定されているコネクションタイプで内部リソースにアクセスすることができます。

注 – *HTML5 VPN ポータル*タブは、管理者がVPNコネクションを作成し、ユーザを許可ユーザに追加している場合にのみ使用可能です。

注 – ブラウザは HTML5 に準拠したものである必要があります。次のブラウザはHTML5 VPN機能をサポートしています : Firefox 6.0以降、Internet Explorer 10以降、Chrome、Safari 5以降、(MACのみ)。

*HTML5 VPN ポータル*タブには、許可されているコネクションのリストが表示されます。アイコンにより、接続のタイプが示されます。

接続を使用するには、次の手順に従います。

1. **それぞれの*接続*ボタンをクリックします。**
   新しいブラウザウィンドウが開きます。その内容とレイアウトは接続タイプに依存します。たとえば、HTTP またはHTTPS 接続を開いた場合には、Webサイトが含まれますが、SSH接続の場合はコマンドラインインタフェースとなります。

2. **新しいVPNウィンドウでの作業。**
   一部のタスクでは、VPNウィンドウは接続タイプに固有のメニューバーを提供します。これは、カーソルがウィンドウの一番上へ移動すると消えます。

   - ファンクションキーまたはキー組合せの使用 : ファンクションキーやCTRL-ALT-DELなどの特殊なコマンドを使用したい場合、*キーボード*メニューでそれぞれのエントリを選択する必要があります。

   - ローカルホストから**VPN** ウィンドウへ、コピー **&** ペーストします : ローカルマシンでは、それぞれのテキストをクリップボードにコピーする必要があります。接続ウィンドウで、*クリップボード*メニューを選択する必要があります。CTRL-Vで、テキストをテキストボックスにペーストします。その後、*サーバに保存*ボタンをクリックする必要があります。SSH またはTelnetによる接続では、テキストを直接カーソル位置へペーストすること

ができます。RDP またはVNC による接続では、テキストはサーバのクリップボードへ送信され、その後通常通りペーストできます。

注 **–** コピー&ペーストはWebapp接続では動作しません。

- **PN** ウィンドウから他のウィンドウへのコピー **&** ペースト: SSH およびTelnetによる接続では、ローカルのWindowsの場合と同様にコピー・アンド・ペーストを行うことができます。RDPまたはVNC による接続では、VPNウィンドウで、それぞれのテキストをクリップボードへコピーする必要があります。次に、*クリップボード*メニューを選択します。コピーしたテキストが、テキストボックスに表示されます。テキストをマークして、`CTRL-C`を押す必要があります。これで、ローカルのクリップボードにコピーされ、通常通りペーストを行うことができます。

- リモートデスクトップ接続でのキーボードレイアウトの変更 : Windowsホストによるリモートデスクトップ接続では、VPNウィンドウのキーボード言語の設定を変更することができます。特にWindowsログインの場合は、パスワードを正確にタイプしていることを確認するために、選択言語がWindowsの言語設定と一致する必要があります。*キーボード*> *キーボードレイアウト*メニューで、適切な言語を選択します。選択したキーボードレイアウトは、cookieに保存されます。

- **Webapp**接続のスタートページに戻る: Webapp接続のデフォルトページに戻るには、*ナビゲーション* > *ホーム*メニューを選択します。

3. **作業終了後の接続の完了。**
    - 最終的に接続を終了するには、*接続*メニューから*セッションの停止*コマンドを選択するか、タイトルバーのXアイコンをクリックしてブラウザウィンドウを閉じます。*接続*ボタンを再度使用して新規セッションを開始することができます。
    - セッションを切断するには、*接続*メニューから*一時停止セッション*コマンドを選択します。セッションのステータスは5分間にわたって保存されます。この時間内に再接続すると、以前のセッションを継続できます。

20.11 ユーザポータル: パスワードの変更

このタブでは、エンドユーザはユーザポータルにアクセスするためのパスワードと、使用できる場合は、PPTPを介したリモートアクセス用のパスワードを変更できます。

20.12 ユーザポータル:HTTPSプロキシ

このタブで、エンドユーザはHTTP/SプロキシCA証明書をインポートし、セキュアなWebサイトへの訪問時に表示されるエラーメッセージを回避することができます。

注 – ユーザポータルの*HTTPSプロキシ*タブは、管理者によってHTTP/Sプロキシの証明書がグローバルに提供されている場合にだけ使用できます。

*プロキシCA証明書をインポート*をクリックすると、ユーザのブラウザに、さまざまな目的でCAを信頼するか確認するプロンプトが表示されます。

用語集

3

3DES
Triple Data Encryption Standard トリプルデータ暗号化標準

A

ACC
Astaro Command Center

ACPI
Advanced Configuration and Power Interface アドバンスドコンフィギュレーションアンドパワーインタフェース

AD
Active Directory

Address Resolution Protocol (アドレス解決プロトコル)
ホストの IP アドレスしかわからない場合に、そのイーサネットMAC アドレスを確定するために使用される。

ADSL
Asymmetric Digital Subscriber Line 非対称デジタル加入者線

Advanced Configuration and Power Interface (アドバンスドコンフィグレーションアンドパワーインタフェース)
ACPI とは電力管理標準の1つであり、コンピュータ内の各デバイスに分散させる電力量をオペレーティングシステムで制御できるようにするものです。

Advanced Programmable Interrupt Controller (アドバンスドプログラマブルインタラプトコントローラ)
マルチプロセッサコンピュータシステムでの割り込みを処理するアーキテクチャ。

AES
Advanced Encryption Standard 高度暗号化標準

AFC
Astaro Flow Classifier

AH
Authentication Header 認証ヘッダ

AMG
Astaro Mail Gateway

APIC
Advanced Programmable Interrupt Controller アドバンスドプログラマブルインタラプトコントローラ

ARP
Address Resolution Protocol アドレス解決プロトコル

AS
Autonomous System 自律システム

ASCII
American Standard Code for Information Interchange 情報交換用米国標準コード

ASG
Astaro Security Gateway

Astaro Command Center
複数の Astaro ゲートウェイ装置を1つのインタフェースで監視管理するためのソフ

トウェア。バージョン4より、Sophos UTM Manager (SUM) に名前が変更されました。

Astaro Security Gateway
メールとWebセキュリティを含む、統合脅威管理のためのソフトウェア。バージョン9より、Unified Threat Management (UTM) に名前が変更されました。

Authentication Header (認証ヘッダ)
アンチリプレイを提供し、伝送中にパケットの内容が改ざんされていないことを検証するIPSecプロトコル。

Autonomous System (自律システム)
1つのエンティティによって管理されるIPネットワークとルータの集合体であり、インターネットに対して共通のルーティングポリシーを持つ。

AWG
Astaro Web Gateway

AWS
Amazon Web Services

B

BATV
Bounce Address Tag Validation バウンスアドレスタグ検証

BGP
Border Gateway Protocol ボーダーゲートウェイプロトコル

Bounce Address Tag Validation (バウンスアドレスタグ検証)
Eメールメッセージに指定された返信アドレスが有効であるかどうかを判定するために規定された手法の名前。偽造された返信アドレスへのバウンスメッセージを拒否するように設計されている。

C

CA
Certificate Authority 認証局

CBC
Cipher Block Chaining 暗号ブロック連鎖

CDMA
Code Division Multiple Access 符号分割多重アクセス

Certificate Authority 認証局
他のパーティによって使用されるデジタル証明書を発行する団体または組織。

CHAP
Challenge-Handshake Authentication Protocol チャレンジハンドシェイク認証プロトコル

Cipher Block Chaining (暗号ブロック連鎖)
暗号処理モードの1つであり、平文 (プレーンテキスト) の各ブロックを直前の暗号文ブロックと「排他的論理和 (XOR)」してから暗号化する。これにより、暗号文の各ブロックはその時点までのすべての平文ブロックに依存するようになる。

CMS
Content Management System コンテンツ管理システム

CPU
Central Processing Unit 中央処理装置

CRL
Certificate Revocation List 証明書失効リスト

CSS
Cascading Style Sheets カスケーディングスタイルシート

D

DC
Domain Controller ドメインコントローラ

DCC用
Direct Client Connection 直接クライアント接続

DDoS
Distributed Denial of Service 分散型サービス拒否

DER
Distinguished Encoding Rules 識別符号化規則

Destination Network Address Translation (宛先ネットワークアドレス変換)
データパケットの宛先アドレスを書き換える特殊なNAT。

DHCP
Dynamic Host Configuration Protocol ダイナミックホスト設定プロトコル

Digital Signature Algorithm (デジタル署名アルゴリズム)
米国連邦政府が推奨しているデジタル署名についての標準 (FIPS)。

Digital Subscriber Line (デジタル加入者線)
地域電話網のケーブル上でのデジタルデータ伝送を提供する技術群。

Distinguished Encoding Rules (識別符号化規則)
X.509証明書などデジタル署名または署名が検証されるデータオブジェクトを符号化するための方式。

DKIM
Domain Keys Identified Mail ドメインキー識別メール

DMZ
Demilitarized Zone 非武装地帯

DN
Distinguished Name 識別名

DNAT
Destination Network Address Translation 宛先ネットワークアドレス変換

DNS
Domain Name Service ドメインネームサービス

DOI
Domain of Interpretation 解釈ドメイン

Domain Name Service (ドメインネームサービス)
インターネットを介して接続されたコンピュータの基底のIPアドレスを、人にとってわかりやすい名前やエイリアスに変換する。

DoS
Denial of Service サービス拒否

DSA
Digital Signature Algorithm デジタル署名アルゴリズム

DSCP
Differentiated Services Code Point 差別化サービスコードポイント

DSL
Digital Subscriber Line デジタル加入者線

DUID
DHCP Unique Identifier DHCP固有識別子

Dynamic Host Configuration Protocol (ダイナミックホスト設定プロトコル)
ネットワーク上のデバイスがIPアドレスを取得するために使用するプロトコル。

E

eBGP
Exterior Border Gateway Protocol エクステリア境界ゲートウェイプロトコル

ECN
Explicit Congestion Notification 明示的な輻輳通知

Encapsulating Security Payload (カプセル化セキュリティペイロード)
データの機密性(暗号)、アンチリプレイ、認証を提供するIPSecプロトコル。

ESP
Encapsulating Security Payload カプセル化セキュリティペイロード

Explicit Congestion Notification (明示的な輻輳通知)
明示的な輻輳通知(ECN)とはインターネットプロトコルの拡張であり、ネットワーク輻輳のエンドツーエンドな通知をパケットのドロップなしで許可します。ECNは、接続の両エンドポイントの間で使用のネゴシエートが成功している場合にのみ機能します。

F

FAT
File Allocation Table ファイルアロケーションテーブル

File Transfer Protocol (ファイル転送プロトコル)
パケット交換網上でのファイル交換用プロトコル。

FQHN
Fully Qualified HostName 完全修飾ホスト名

FTP
File Transfer Protocol ファイル転送プロトコル

G

Generic Routing Encapsulation (ジェネリックルーティングカプセル化)
任意のネットワーク層パケット内で任意のネットワーク層パケットをカプセル化するために規定されたトンネリングプロトコル。

GeoIP
衛星画像を使用して世界中のデバイスの位置を特定する技術。

GRE
Generic Routing Encapsulation ジェネリックルーティングカプセル化

GSM
Global System for Mobile Communications 汎欧州デジタル移動電話方式

H

HA
High Availability 高可用性

HCL
Hardware Compatibility List ハードウェア互換性リスト

HELO
SMTP Simple Mail Transfer Protocol: 簡易メール転送プロトコル のコマンドであり、クライアントはこれを使用してサーバーからの初期グリーティングに応答します。

High Availability 高可用性
信頼できるレベルの運用継続性を確実に保証するためのシステム設計プロトコル。

HIPS
Host-based Intrusion Prevention System ホストベースの侵入防止システム

HMAC
Hash-based Message Authentication Code ハッシュベースのメッセージ認証コード

HTML
Hypertext Transfer Markup Language ハイパーテキスト転送マークアップ言語

HTTP
Hypertext Transfer Protocol ハイパーテキスト転送プロトコル

HTTP over SSL
よりセキュアなHTTP通信を実現するプロトコル。

HTTP/S
Hypertext Transfer Protocol Secure ハイパーテキスト転送プロトコルセキュア

HTTPS
Hypertext Transfer Protocol Secure ハイパーテキスト転送プロトコルセキュア

Hypertext Transfer Protocol (ハイパーテキスト転送プロトコル)
インターネット上で情報を転送するためのプロトコル。

I

IANA
Internet Assigned Numbers Authority インターネット番号割当当局

iBGP
Interior Border Gateway Protocol インテリア境界ゲートウェイプロトコル

ICMP
Internet Control Message Protocol インターネット制御メッセージプロトコル

ID
Identity アイデンティティ

IDE
Intelligent Drive Electronics インテリジェントドライブエレクトロニクス

IDENT
特定のTCP接続のユーザーを特定するための標準プロトコル。

IDN
International Domain Name 国際ドメイン名

IE
Internet Explorer

IKE
Internet Key Exchange インターネット鍵交換

IM
Instant Messaging インスタントメッセージング

Internet Control Message Protocol (インターネット制御メッセージプロトコル)
ネットワークのステータスやその他のコントロール情報についての情報を送受信するために使用される特別なIPプロトコル。

Internet Protocol (インターネットプロトコル)
パケット交換網上でのデータ通信に使用されるデータ指向プロトコル。

Internet Relay Chat (インターネットリレーチャット)
インターネット上でのインスタント通信を可能にするオープンプロトコル。

IP
Internet Protocol インターネットプロトコル

IPS
IPS 侵入防御システム

IPsec
Internet Protocol Security インターネットプロトコルセキュリティ

IPアドレス
インターネットプロトコル標準を使用するコンピュータネットワーク上の各デバイスが互いを特定し、通信するために使用する一意の番号。

IRC
Internet Relay Chat インターネットリレーチャット

ISP
Internet Service Provider インターネットサービスプロバイダ

L

L2TP
Layer Two (2) Tunneling Protocol レイヤ2トンネリングプロトコル

LAG
Link Aggregation Group リンクアグリゲーショングループ

LAN
Local Area Network ローカルエリアネットワーク

LDAP
Lightweight Directory Access Protocol ライトウェイトディレクトリアクセスプロトコ

ル

Link-state advertisement (リンクステートアドバタイズメント)
IP用のOSPFルーティングプロトコルの基本的な通信手段。

LSA
Link-state advertisement リンクステートアドバタイズメント

LTE
3GPP Long Term Evolution 3GPPロングタームエボリューション

M

MAC
Media Access Control メディアアクセスコントロール

MAC アドレス
ほとんどの形態のネットワークハードウェアに割り当てられる一意のコード。

Management Information Base (管理情報ベース)
通信ネットワーク内のデバイスを管理するために使用されるデータベースの種類。ネットワーク内のエンティティ(ルータやスイッチなど)を管理するために使用される(仮想)データベース内のオブジェクトの集合から構成される。

Masquerading
LAN全体で1つのパブリックIPアドレスを使用してインターネットの他の部分と通信できるようにするNATベースの技術。

MD5
Message-Digest algorithm 5 メッセージダイジェストアルゴリズム5

Message-Digest algorithm 5 (メッセージダイジェストアルゴリズム5)
128ビットのハッシュ値による暗号ハッシュ関数。

MIB
Management Information Base 管理情報ベース

MIME
Multipurpose Internet Mail Extensions 多目的インターネットメール拡張

MPLS
Multiprotocol Label Switching マルチプロトコルラベルスイッチング

MPPE
Microsoft Point-to-Point Encryption マイクロソフトポイントツーポイント暗号化

MSCHAP
Microsoft Challenge Handshake Authentication Protocol マイクロソフトチャレンジハンドシェイク認証プロトコル

MSCHAPv2
Microsoft Challenge Handshake Authentication Protocol Version 2 マイクロソフトチャレンジハンドシェイク認証プロトコルバージョン2

MSP
マネージドサービスプロバイダ

MSSP
マネージドセキュリティサービスプロバイダ

MTU
Maximum Tansmission Unit 最大伝送単位

Multipurpose Internet Mail Extensions (多目的インターネットメール拡張)
Eメールのフォーマットを拡張し、US-ASCII以外の文字セットのテキスト、テキスト以外の添付物、マルチパートメッセージ本体、ASCII以外の文字セットでのヘッダ情報をサポートするためのインターネット標準。

MX レコード
インターネットでEメールをどのようにルーティングするのかを指定する、ドメインネームシステム DNS 内のリソースレコードの種類。

N

NAS
Network Access Server ネットワークアクセスサーバー

NAT
Network Address Translation ネットワークアドレス変換

NAT-T
NAT Traversal NAT トラバーサル

Network Address Translation (ネットワークアドレス変換)
IP アドレスを再利用するためのシステム。

Network Time Protocol (ネットワークタイムプロトコル)
パケット交換網上でコンピュータシステムのクロックを同期するためのプロトコル。

NIC
Network Interface Card ネットワークインタフェースカード

Not-so-stubby area (Not-so-stubby エリア)
OSPF プロトコルの中で、自律システム (AS) 外部ルートをインポートし、それらをバックボーンに送信することはできるが、バックボーンやその他のエリアからAS外部ルートを受信することはできないタイプのスタブエリア。

NSSA
Not-so-stubby area Not-so-stubbyエリア

NTLM
NT LAN Manager Microsoft Windows

NTP
Network Time Protocol ネットワークタイムプロトコル

O

Open Shortest Path First (オープンショーテストパスファースト)
ネットワークルーティングのための、リンクステート型の階層的な IGP (interior gateway protocol)。

OpenPGP
強力な公開鍵と対称暗号を組み合わせて、電子通信とデータストレージのためのセキュリティサービスを提供するプロトコル。

OSI
Open Source Initiative オープンソースイニシアチブ

OSPF
Open Shortest Path First オープンショーテストパスファースト

OU
Organisational Unit 組織単位

P

PAC
プロキシ自動設定

PAP
Password Authentication Protocol パスワード認証プロトコル

PCI
Peripheral Component Interconnect ペリフェラルコンポーネントインターコネクト

PEM
Privacy Enhanced Mail プライバシー拡張メール

PGP
Pretty Good Privacy プリティグッドプライバシー

PKCS
Public Key Cryptography Standards 公開鍵暗号標準

PKI
Public Key Infrastructure 公開鍵暗号基盤

PMTU
Path Maximum Transmission Unit パス最大伝送単位

POP3
Post Office Protocol version 3 ポストオフィスプロトコルバージョン3

Post Office Protocol version 3 (ポストオフィスプロトコルバージョン3)
パケット交換網上でEメールを配信するためのプロトコル。

PPP
Point-to-Point Protocol ポイントツーポイントプロトコル

PPPoA
PPP over ATM Protocol PPPオーバーATMPプロトコル

PPTP
Point to Point Tunneling Protocol ポイントツーポイントトンネリングプロトコル

Privacy Enhanced Mail (プライバシー拡張メール)
公開鍵暗号を使用してEメールのセキュリティを保護するための、初期のIETF提案。

PSK
事前共有鍵 Preshared Key

Q

QoS
Quality of Service サービス品質

R

RADIUS
Remote Authentication Dial In User Service リモート認証ダイヤルインユーザーサービス

RAID
Redundant Array of Independent Disks 独立ディスク冗長アレイ

RAM
Random Access Memory ランダムアクセスメモリ

RAS
Remote Access Server リモートアクセスサーバー

RBL
Realtime Blackhole List リアルタイムブラックホールリスト

RDN
Relative Distinguished Name 相対識別名

RDNS
Reverse Domain Name Service リバースドメインネームサービス

RDP
Remote Desktop Protocol リモートデスクトッププロトコル

RED
リモートイーサネットデバイス

Redundant Array of Independent Disks (独立ディスク冗長アレイ)
複数のハードドライブを使用してドライバ間でデータを共有または複製するデータ保管スキーム。

Remote Authentication Dial In User Service (リモート認証ダイヤルインユーザーサービス)
ルータなどのネットワークデバイスが中央データベースに対してユーザーを認証できるように設計されたプロトコル。

RFC
Request for Comment リクエストフォーコメント

RPS
REDプロビジョニングサービス

RSA
Rivest, Shamir, & Adleman リベスト、シャミア、エーデルマン: 公開鍵暗号化技術

S

S/MIME
Secure/Multipurpose Internet Mail Extensions セキュア多目的インターネットメール拡張

SA
Security Associations セキュリティアソシエーション

SAA
Sophos Authentication Agent ソフォス認証エージェント

SCP
Secure Copy セキュアコピー: セキュア通信用のSSHコンピュータアプリケーションスイートからの

SCSI
Small Computer System Interface スモールコンピュータシステムインタフェース

Secure Shell (セキュアシェル)
異なるパケット交換網にまたがるローカルコンピュータとリモートコンピュータの間で

セキュアなチャネルを確立するためのプロトコル。

Secure Sockets Layer (セキュアソケットレイヤ)
インターネット上でセキュアな通信を提供する暗号プロトコル。TLS (トランスポートレイヤセキュリティ) の前身である。

Secure/Multipurpose Internet Mail Extensions (セキュア多目的インターネットメール拡張)
MIMEにカプセル化されたEメールに対する公開鍵暗号化や署名のための標準。

Security Parameter Index (セキュリティパラメータインデックス)
IP トラフィックのトンネリングにIPSec を使用するときにヘッダに追加される識別タグ。

Sender Policy Framework (送信者ポリシーフレームワーク)
SMTP (Simple Mail Transfer Protocol: 簡易メール転送プロトコル) の拡張。SPFを使用すると、スパムによく見られるSMTP MAIL FROM リターンパス の偽造アドレスをソフトウェアで特定し、拒否することができる。

Session Initiation Protocol (セッション開始プロトコル)
2つ以上の通信パートナー間でセッションを確立、変更、終了するためのシグナリングプロトコル。このテキスト指向のプロトコルは HTTP をベースとしており、IP ネットワーク経由でTCPまたは UDP を通して信号データを送信できる。そのため、VoIP (Voice-over-IP) ビデオ電話やリアルタイムなマスチメディアサービスなどの基盤となる。

SFQ
Stochastic Fairness Queuing 確率的不偏キューイング

SIM
Subscriber Identification Module

Simple Mail Transfer Protocol (簡易メール転送プロトコル)
パケット交換網上でEメールを送受信するために使用されるプロトコル。

Single sign-on (シングルサインオン)
ユーザーが一度だけ認証を行い、1つのパスワードを使用して複数のアプリケーションやシステムにアクセスできるようにする認証方式。

SIP
Session Initiation Protocol セッション開始プロトコル

SLAAC
Stateless Address Autoconfiguration ステートレスアドレス自動設定

SMB
Server Message Block サーバーメッセージブロック

SMP
Symmetric Multiprocessing 対称型マルチプロセッシング

SMTP
Simple Mail Transfer Protocol 簡易メール転送プロトコル

SNAT
Source Network Address Translation 送信元ネットワークアドレス変換

SNMP
Simple Network Message Protocol シンプルネットワークメッセージプロトコル

SOCKetS
クライアントサーバーアプリケーションがネットワークファイアウォールのサービスを透過的に使用できるようにするインターネットプロトコル。現在、SOCKS (別名: ファイアウォールトラバースプロトコル) はバージョン5であり、正しく機能するためにはクライアント側のプログラムに導入する必要がある。

SOCKS
SOCKetS

Sophos UTM Manager
複数のUTM装置を1つのインタフェースで監視管理するためのソフトウェア。(旧製品: Astaro Command Center)。

Source Network Address Translation (送信元ネットワークアドレス変換)
特殊なNAT。SNATでは、接続を開始したコンピュータのIPアドレスが書き換えられる。

Spanning Tree Protocol (スパニングツリープロトコル)
ブリッジのループを検出して回避するネットワークプロトコル

SPF
Sender Policy Framework 送信者ポリシーフレームワーク

SPI
Security Parameter Index セキュリティパラメータインデックス

SPX
Secure PDF Exchange

SSH
Secure Shell セキュアシェル

SSID
Service Set Identifier サービスセット識別子

SSL
Secure Sockets Layer セキュアソケットレイヤ

SSO
Single sign-on シングルサインオン

STP
Spanning Tree Protocol スパニングツリープロトコル

SUA
Sophos User Authentication ソフォスユーザー認証

SUM
Sophos UTM Manager

Symmetric Multiprocessing (対称型マルチプロセッシング)
複数CPUを使用すること。

SYN
Synchronous 同期

T

TACACS
Terminal Access Controller Access Control System ターミナルアクセスコントローラアクセスコントロールシステム

TCP
Transmission Control Protocol 伝送制御プロトコル

TFTP
Trivial File Transfer Protocol 簡易ファイル転送プロトコル

Time-to-live (生存時間)
IP (インターネットプロトコル) ヘッダ内の8ビットのフィールドであり、パケットをネットワーク経由で伝送できる制限時間を指定する。この時間が経過すると、そのパケットは廃棄される。

TKIP
Temporal Key Integrity Protocol 一時鍵完全性プロトコル

TLS
Transport Layer Security トランスポートレイヤセキュリティ

TOS
Type of Service サービスタイプ

Transmission Control Protocol (伝送制御プロトコル)
インターネットプロトコルスイートのプロトコル。これにより、ネットワーク内のコンピュータ上のアプリケーションが相互接続できる。このプロトコルによって、データが送信者から受信者へ確実かつ順序通りに送信される。

Transport Layer Security (トランスポートレイヤセキュリティ)
インターネット上でセキュアな通信を提供する暗号プロトコル。SSL (セキュアソケットレイヤ) の後継プロトコルである。

TTL
Time-to-live 生存時間

U

UDP
User Datagram Protocol ユーザーデータグラムプロトコル

UMTS
Universal Mobile Telecommunications System ユニバーサル移動体通信システム

Unified Threat Management
メールとWebセキュリティを含む、統合脅威管理のためのソフトウェア。(旧製品: Astaro Security Gateway)。

Uniform Resource Locator (ユニフォームリソースロケータ)
インターネット上のリソースの位置を指定する文字列。

Up2Date
Sophos サーバーから関連する更新パッケージをダウンロードするためのサービス。

UPS
Uninterruptible Power Supply 無停電電源装置

URL
Uniform Resource Locator ユニフォームリソースロケータ

USB
Universal Serial Bus ユニバーサルシリアルバス

User Datagram Protocol (ユーザーデータグラムプロトコル)
ネットワーク上のコンピュータのアプリケーションで短いメッセージ (別名: データグラム) をやりとりするためのプロトコル。

UTC
Coordinated Universal Time 協定世界時

UTM
Unified Threat Management

V

VDSL
Very High Speed Digital Subscriber Line 超高速デジタル加入者線

Virtual Private Network (バーチャルプライベートネットワーク)
公衆通信インフラを利用するプライベートデータネットワーク。PPTP や IPSec などのトンネリングプロトコルを使用してプライバシーを維持する。

VLAN
Virtual LAN バーチャルLAN

VNC
Virtual Network Computing 仮想ネットワークコンピューティング

Voice over IP (ボイスオーバー IP)
インターネット上またはその他の IP ベースのネットワーク上での音声会話ルーティング。

VoIP
Voice over IP ボイスオーバーIP

VPC
Virtual Private Cloud バーチャルプライベートクラウド

VPN
Virtual Private Network バーチャルプライベートネットワーク

W

WAF
Web アプリケーションファイアウォール

WAN
Wide Area Network ワイドエリアネットワーク

W-CDMA
Wideband Code Division Multiple Access 広帯域符号分割多重アクセス

WebAdmin
UTM、SUM、ACC、ASG、AWG、および AMG などの Sophos/Astaro 製品用の Web ベース GUI。

WEP
Wired Equivalent Privacy 有線同等機密

Windows Internet Naming Service (Windowsインターネットネーミングサービス)
マイクロソフトが Windows に実装した NBNS (NetBIOS Name Server: NetBIOS ネームサーバー)。NetBIOS コンピュータ名のためのネームサーバーおよびサービスである。

WINS
Windows Internet Naming Service　Windowsインターネットネーミングサービス

WLAN
Wireless Local Area Network　無線LAN

WPA
Wi-Fi Protected Access　Wi-Fi保護アクセス

X

X.509
ITU-T (国際電気通信連合、電気通信標準化部門) が公開したデジタル証明書の仕様。個人またはコンピュータシステムの識別に必要な情報や属性を規定する。

XSS
Cross-site scripting　クロスサイトスクリプティング

イ

インターネットサービスプロバイダ
インターネットや関連サービスへのアクセスを利用者に販売する企業または組織。

ク

クラスタ
リンクされたコンピュータのグループ。緊密に連携して多くの局面で1台のコンピュータとして機能する。

サ

サブネットマスク
ネットワークのサブネットマスク(別名: ネットマスク) とネットワークアドレスによって、ローカルネットワークの一部となるアドレスとならないアドレスが定義される。個々のコンピュータは、この定義に基づいてネットワークに割り当てられる。

デ

デバイスツリー
メインメニューの下にあり、SUM に登録されたすべてのゲートウェイ装置にアクセス権を付与する。

ブ

ブロードキャスト
ネットワーク内の他のすべてのコンピュータに向けてメッセージを一括送信するためにコンピュータで使用されるアドレス。たとえば、IP アドレスが 192.168.2.0 でネットワークマスクが 255.255.255.0 のネットワークは、ブロードキャストアドレスが 192.168.2.255 となる。

プ

プロキシ
クライアントが他のネットワークサービスに対して間接的にネットワーク接続できるようにするコンピュータネットワークサービスを提供するコンピュータ。

プロトコル
2つのコンピュータエンドポイント間での接続、通信、データ転送を制御または実現するための、明確で標準化されたルールセット。

ポ

ポート

データを直接交換するためにプログラムで使用できる仮想データ接続。具体的には、ポートとは追加の識別子である(TCP とUDP の場合、0～65535 の番号)。これにより、コンピュータはある2台のコンピュータ間に存在する複数の同時接続を見分けることができる。

ポートスキャン

ネットワークホストの空きポートを探す行為。

マ

マネージドセキュリティサービスプロバイダ

企業に対してセキュリティサービスを提供する。

リ

リアルタイムブラックホールリスト

スパム行為に関与しているIP アドレスのリストをインターネットサイトが公開できる手段。ほとんどのメール転送エージェント(メールサーバー) ソフトウェアは、1つ以上のブラックホールリストに記載されたサイトから送信されたメッセージを拒否したりフラグを付加したりするように設定できる。Web サーバーも、RBL に掲載されているクライアントを拒否することができます。

ル

ルータ

最も効率の良いパスで宛先までパケットを転送するために指定されるネットワークデバイス。

共

共有シークレット

セキュア通信の2つのエンティティ間で共有されているパスワードまたはパスフレーズ。

無

無停電電源装置

接続された機器に対する継続的な配電を維持するためのデバイス。通常電源を使用できないときには別の電源から電力を供給する。

図のリスト